PERFORMANCE INVESTIGATION OF SECURE

802.11 WIRELESS LANS:

Raising the Security Bar to Which Level?

A thesis

submitted in partial fulfilment

of the requirements for the Degree

of

Master of Commerce in

Accountancy, Finance, and Information Systems

in the

University of Canterbury

by

Jenne Wong

University of Canterbury

2003

Acknowledgments

I would like to thank my supervisors, Dr John Vargo and Associate Professor Ray Hunt, who have provided me with invaluable answers to my questions and guidance in the preparation of this thesis.

I would like to acknowledge all the support and encouragement given by my family and friends. Each of you have contributed in your own special way, and helped me during difficult times.

I would like to express also my most sincere thanks to Peter Davison, for providing me with wireless technical support. I would also like to thank Dr. Paul Cragg for statistical guidance, Chris Harrow for Windows operating system management directions, and Chris Rodgers for experiment setup discussions.

Finally, thanks to Lucent Technologies, Telecom Mobile, MediaLab, and the Government Communications Security Bureau for providing me the opportunity to perform this research.

Jenne Wong
2003

Abstract

Wireless networks have gained popularity, providing users flexibility and mobility in accessing information. The IEEE 802.11 Wireless Local Area Network (WLAN) standard has become the dominant architecture in practice. Private WLANs are used by businesses and home users, while public WLANs have been established in areas expected to have high demand for bandwidth, such as cafes, airports, and hotels.

Existing solutions for such WLAN access networks have been exposed to security vulnerabilities. Although researchers have proposed improved security for WLANs, very little work exists in the area of understanding the interaction between WLANs and their emerging and evolving security architectures with respect to the performance impacts of these security measures. The aim of this thesis is to quantify the impact on network performance resulting from the adoption of these security mechanisms.

This study investigated the performance and security issues of IEEE 802.11 wireless networks using layered security models. The two models defined in the research were the IEEE 802.1X and Virtual Private Network (VPN). Our results showed that different security mechanisms degraded WLAN performance in different ways. Network performance degradation increased as the protection of the security mechanisms increased. Furthermore, the VPN model impacted the performance more than the 802.1X model. The performance degradation calculated was incorporated into constructing a wireless security policy template for wireless “security insurance”.

Table of Content

List of Figures

List of Tables

CHAPTER 1

Introduction

Wireless networks are emerging as a significant aspect of networking; *wireless local area networks* (WLANs, see Acronyms and Abbreviations), Bluetooth, and cellular systems have become increasingly popular in the business and computer industry, with consequent security issues. WLANs, especially the *Institute of Electrical and Electronics Engineers* (IEEE) 802.11 networks, are becoming common access networks in private and public environments. The freedom of movement and simplicity in its implementation have made WLANs popular in the home and businesses sectors, as well as hotspots[1] such as airports and cafes. The increasing availability of, and therefore increasing reliance on, wireless networks makes it extremely important to maintain reliable and secure communications in the wake of network component failures or security breaches. However, recent news reports on a number of attacks against wireless networks, especially WLANs, have alarmed wireless adopters, developers, and intended users. The broadcast nature of wireless communication links makes them unique in their vulnerability to security attacks and their susceptibility to intentional threats. Organisations that want to deploy a secured WLAN infrastructure are challenged by the flaws in the existing wireless mechanism design, such as the *wired equivalent privacy* (WEP) protocol.

Although researchers have proposed improved security for WLANs, very little work exists in the area of understanding the interaction between WLANs and their emerging and evolving security architectures with respect to the performance impact of these security measures.

This study investigated the performance and security issues of IEEE 802.11 wireless networks using layered security models. These models, such as 802.1X and *virtual private network* (VPN), were selected from a variety of proposed security mechanisms. This study consisted of a performance evaluation with layered security

[1] Hotspots are a form of public WLAN allowing users to access Internet from any WLAN structures.

implementations to provide us with a set of possible operating and management parameters. These parameters would be incorporated into secure wireless network management policies.

1.2 Problem Statement

The industry accepts security mechanisms such as encryption, authentication, and other techniques as requirements in a wired network. However, there is very little information on the performance costs associated with implementing these processes in a wireless network. Furthermore, there is no analysis on how well a wireless network integrates with traditional security mechanisms such as a firewall, authentication, and encryption.

The practicality of any security policy depends on whether that policy is enforceable and at what cost. Prior research has emphasised mechanisms to enforce network security, yet the importance of security "cost" on performance and management has not been evaluated. The aim of this research is to determine performance and security issues in wireless networks, and to identify vulnerabilities in the operation of IEEE 802.11 WLANs.

In order to evaluate the impact of security on performance, a testbed was setup to assess existing security technologies and their effects on network performance. *File transfer protocol* (FTP) and *hypertext transfer protocol* (HTTP) are the common application protocols used for data transfer, and were evaluated in conjuction with various security mechanisms. This thesis quantified important performance variables which included response time and throughput for the various application protocols.

1.3 Thesis Outline

Chapter 2 provides an introduction to existing wireless networks. A detailed analysis of the structure and protocols used for IEEE 802.11b is presented. Chapter 3 discusses security threats and mechanisms to mitigate such risks. Various security architectures, ranging from existing 802.11 and 802.1X standards; *authentication, authorisation, and accounting* (AAA) infrastructure; and VPN components are examined. Chapter 4

provides a brief overview of the performance requirements and discusses prior research carried out to evaluate network performance.

Chapter 5 explains the goals that drove the research, the derived requirements, and the way that different security mechanisms were constructed to carry out the experiments. Chapter 6 presents the model and system architectures; it provides readers with the structure of the experiments.

Chapter 7 analyses the data collected during the experiments. Various performance evaluations were carried out on interaction between different models, traffic types, and security level interactions. A wireless security strategy treating security policies as "insurance policies" is proposed in Chapter 8. Scenarios of how security and performance can be incorporated into an insurance policy are given. Chapter 9 concludes our findings and indicates directions for future work.

Appendix A provides an extract of the data collected from our experiments. The operation of system architecture and security mechanisms used for WLAN is demonstrated in Appendix B. Appendix C describes the various formations of the remote access policies used in the experiments. Finally, acronyms and abbreviations are included in the appendices.

CHAPTER 2

Wireless Networks

Wireless technologies enable freedom of mobility for users by releasing the constraint of physical connections – network connections become cable-free. Wireless technologies use *radio frequency* (RF) as the medium of transmission, and allow organisations to eliminate cables for simpler network management at effective costs. The technologies range from complex systems, such as WLANs and cellular networks, to simple devices such as wireless headphones.

In this chapter, a brief overview of different wireless networks is presented, followed by an in-depth discussion of the 802.11 standards and other requirements for wireless networks, such as roaming. The experimental portion of this thesis is however limited to 802.11 and focuses on the infrastructure mode.

2.1 Wireless Networks

Wireless networking comprises different wireless technologies ranging from *wireless wide area network* (WWAN), and *wireless local area network* (WLAN), to *wireless personal area network* (WPAN). These wireless technologies transmit data over different radio frequency bands and speeds to provide different degrees of mobility (Figure 2-1, adapted from Chevillat and Schott [2001]).

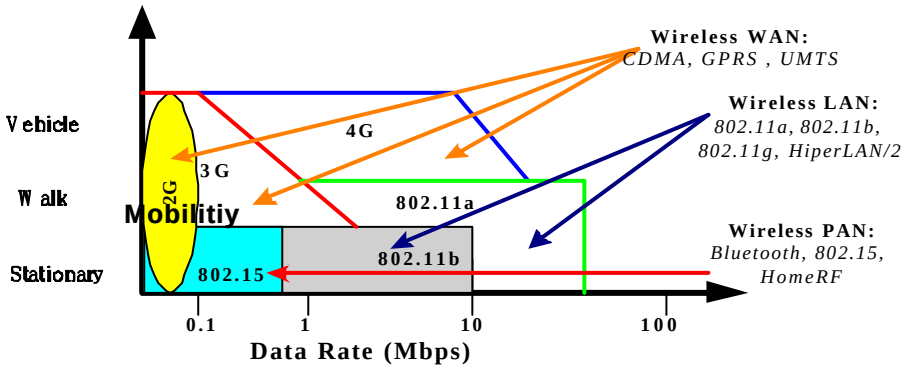

Figure 2-1 Overview of Wireless Networks

2.1.1 Wireless WANs

A WWAN is a computer network that extends over a large geographical area. Characteristically, a WWAN receives and transmits data using radio signals over an interconnection with a mobile computer system. At the mobile switching centre, WWAN segments then connect to either a specialised public or private network via telephone or other high-speed communication link. These back-hauls interconnect and then link to an organisation's existing LAN/WAN infrastructure. Recent developments allow direct connections to generic public networks, such as the Internet, further reducing the cost of deployment. WWANs are normally measured in kilometers, and their data throughput rates are a great deal slower than WLAN connections (typically measured in tens of thousands of bytes per second or slower). The average access speed can be slower than a 28.8 Kbps modem connection. In general, wireless networks are also more susceptible to environmental factors, such as weather, than wired networks.

WWANs encompass a variety of standards. The *Advanced Mobile Phone Systems* (AMPS) standard, which governed *first-generation* (1G) mobile telephone devices, allowed interoperable wireless network infrastructure among vendors. The AMPS standard uses *Frequency Division Multiple Access* (FDMA) and requires a great deal of bandwidth while operating in the 824–829 MHz range. Other telephony standards include the *Time Division Multiple Access* (TDMA) standard, and the *Code Division Multiple Access* (CDMA) standard. Existing *second-generation* (2G) digital cellular systems are *Global System for Mobile* (GSM) in Europe, and *Personal Digital Communication* (PDC) in Japan. *General Packet Radio System* (GPRS) belongs to GSM 2.5G. The 2G to 2.5G wireless WANs provides data rate from 9.6 Kbps to 348 Kbps. As for *third-generation* (3G) systems, *Universal Mobile Telecommunication System* (UMTS) is one of the major systems aiming for higher capacity and data rates with global mobility, and operates around 144 Kbps to 2 Mbps [Hannikainen et al., 2002].

2.1.2 Wireless LANs

WLANs provide greater flexibility and scalability than traditional LANs. Unlike a wired LAN, which requires a wire to access the network, a WLAN facilitates network

transmissions of data from computers and other components through an *access point* (AP). An AP typically provides a range (cell or area coverage) of 100 metres. IEEE 802.11 is an international standard providing transmission speeds ranging from 1 Mbps to 54 Mbps in either the 2.4 GHz or 5 GHz frequency bands. The 802.11b is the dominant WLAN technology at present [WECA, 2001b], and provides an expected data throughput of 5.5 Mbps [Computer Society, 2001; Gast, 2002]. Section 2.2 discusses the 802.11 standard in more detail.

High performance radio LAN (HiperLAN [2002]) is a *European Telecommunications Standards Institute* (ETSI) standard operating in the 5 GHz frequency band; HiperLAN/1 has a transmission speed of 19 Mbps, while HiperLAN/2 operates at 54 Mbps. HiperLAN/2 supports *quality of service* (QoS) and is based on an infrastructure topology, whereas HiperLAN/1 is more suitable for forming ad-hoc networks.

2.1.3 Wireless PANs

WPAN technology emphasises low cost and low power consumption, usually at the expense of range and peak speed. WPANs typically provide a maximum range of 10 meters, facilitating communication between laptops, cell phones, and *personal digital assistants* (PDAs). The best-known WPAN technology, Bluetooth, operates in the 2.4 GHz frequency band at 1 Mbps [SIG, 2000]. Bluetooth users can expect a maximum available speed of approximately 700 Kbps. IEEE 802.15 was formed with a similar goal to Bluetooth. It aims at very low power consumption, and operates at 10 meters with data rates less than 1 Mbps. The 802.15 WPAN standard targets interoperability between WPAN devices, and devices meeting the IEEE 802.11 standard [Hannikainen et al., 2002]. Research is in process to provide WPAN with higher transmission rates up to 10 Mbps, including the development of Bluetooth 2 and IEEE 802.15 *task group* (TG) 3.

HomeRF [2002] is another WPAN technology operating over a common wireless interface at 1-, 2-, and 10-Mbps data rates in the 2.4 GHz band for wireless digital communication between PCs and consumer electronic devices for home and small businesses. Infrared communication is limited due to line-of-sight requirements between the transmitter and the receiver.

2.2 IEEE 802.11 Standards

The IEEE ratified the 802.11 standard in October 1997 [IEEE Std. 802.11b, 1999], and revised it in March 1999. The standard provides three *physical* (PHY) layers and one *medium access control* (MAC) layer for deploying wireless communication in local networks (Figure 2-2, adapted from Held [2001]). As for the *logical link control* (LLC) layer, there is no difference between wireless (802.11) and wired (802) LANs, such as the IEEE 802.3 Ethernet network. The MAC protocol provides two service types (see Section 2.2.3): asynchronous using the *distributed coordination function* (DCF), and synchronous using the *point coordination function* (PCF) that is contention-free.

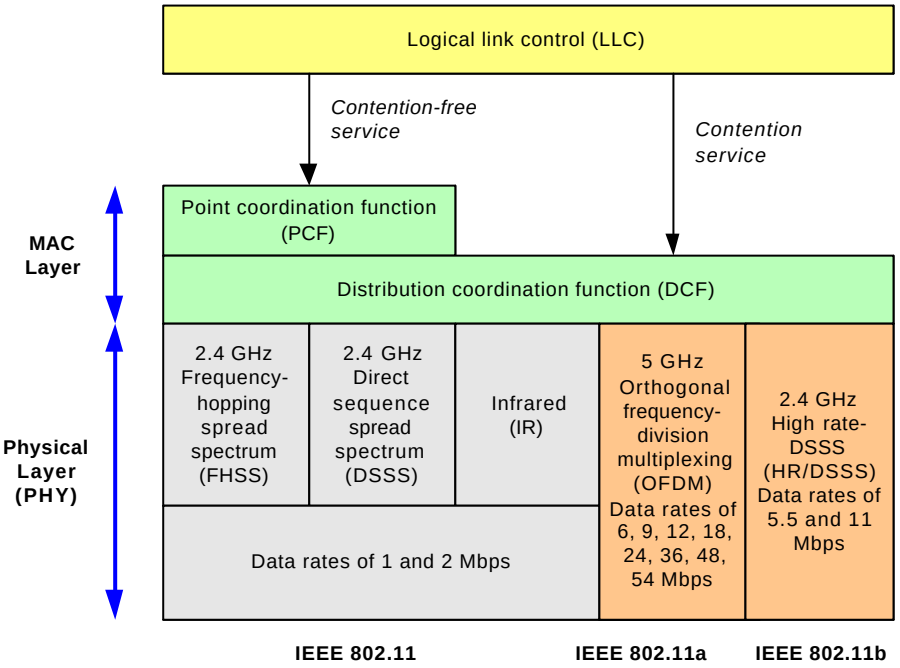

Figure 2-2 The 802.11 Protocol Stack

The 802.11 standard is a family of specifications originally providing a 1 to 2 Mbps data transmission rate using either the *frequency-hopping spread spectrum* (FHSS) or *direct sequence spread spectrum* (DSSS); see Section 2.2.2 for more detail. After revisions, the standard includes 802.11a, operating in a 5 GHz frequency band at 54 Mbps, and 802.11b and IEEE 802.11g, operating in a 2.4 GHz frequency band at speeds of 11 Mbps and 54 Mbps, respectively [O'Hara & Petrick, 1999].

The 802.11 standard takes advantage of radio spectrum technologies, allowing multiple users to share the radio frequencies without end-user licenses. Specifically, it makes uses of the 2.4 GHz *Industrial, Scientific, and Medical* band (ISM) band for 802.11 and 802.11b networks, and the 5 GHz *Unlicensed National Information Infrastructure* (UNII) band for 802.11a-based networks. The *International Telecommunication Union* (ITU) defines both bands. However, interference issues remain, especially in the 2.4 GHz band; if the technology interferes with an authorised operation such as an airline radio frequency, it will cease to operate. In addition, there is no protection from other technologies, such as Bluetooth, accessing 802.11 frequencies.

2.2.1 Architecture Components

The architecture of 802.11 is composed of cells, which can overlap. The *basic service set* (BSS) represents the coverage area of an individual cell, and outside the BSS, a *station* (STA, such as a mobile client) cannot communicate with stations in this cell. The 802.11 standards operate in two modes (Figure 2-3, adapted from ANSI/IEEE 802.11 Std. [1999]): *infrastructure mode* (also known as BSS), and ad-hoc mode or *independent BSS* (IBSS).

The ad-hoc mode is composed solely of clients within a mutual communication range via the wireless medium; it is formed in a spontaneous manner and exists for a limited time in a small area. Examples of ad-hoc networks include rescue operations, conferences, and military operations. The coverage area is composed of the overlapping coverage area of each client.

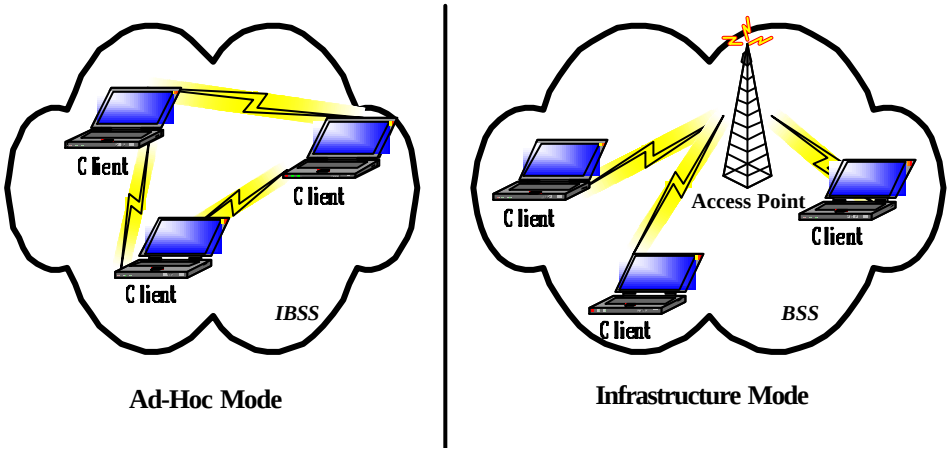

Figure 2-3 Ad-Hoc and Infrastructure Modes

In the infrastructure mode, all wireless clients' communications are passed through a central station, an AP, which manages the network flow and access. The AP provides functionality similar to that provided by a base station in other cellular networks because it acts as a bridge between the wireless segment and the wired segment. This architecture allows for the interconnection of several (infrastructure) BSSs, which form an *extended service set* (ESS, see Figure 2-4; adapted from [ANSI/IEEE Std. 802.11, 1999]). An ESS is built by connecting several APs through a backbone network called a *distribution system* (DS). For example, an 802.3 or Ethernet segment is a DS. The AP defines the coverage area. A *portal* is a logical point, which is required to integrate the 802.11 architecture with existing wired LANs facilitating the transmission. An AP with software implementation can offer the portal service.

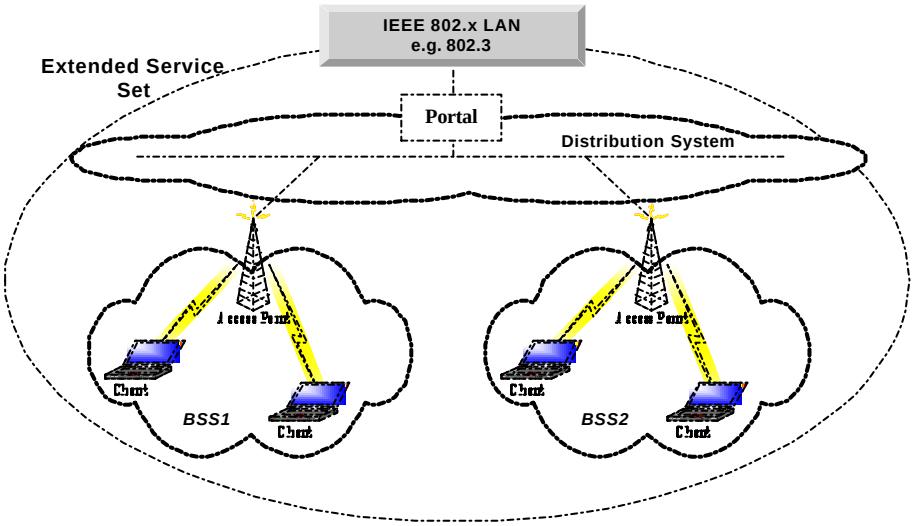

Figure 2-4 ESS

2.2.2 Physical Layers

The physical layer processes data to and from radio signals over the airwave. In other words, it handles the transmission of the frame via the air interface. The standards define five alternative physical layers (Figure 2-2):

- Frequency-hopping spread spectrum (FHSS)
- Direct sequence spread spectrum (DSSS)
- High-rate direct sequence spread spectrum (HR/DSSS)
- Orthogonal frequency-division multiplexing (OFDM)
- Infrared (IR)

The first three physical layers belong to radio spread spectrum technology that operates in the 2.4 GHz band, while OFDM operates in the 5 GHz band. IR operates in the 300-428 GHz band and operates at a slow speed with line-of-sight connection. IR has become a legacy protocol thus will not be addressed in this discussion.

2.2.2.1 FHSS

FHSS modulates data signals with a carrier signal that hops from one frequency to another, using time as its measurement, over a wide range of frequencies. The carrier frequency (between 2.4 and 2.483 GHz) is changed periodically to avoid collisions. A collision occurs only when both a narrowband system and the spread spectrum signals are transmitting at the same frequency simultaneously. A hopping code is used to decide the order of data transmission and which frequency to hop to. FHSS provides a maximum data transmission speed of 2 Mbps.

2.2.2.2 DSSS and HR/DSSS

DSSS combines a data signal at the sending station with a higher data rate bit sequence, known as the chipping code or processing gain. This chipping code reduces interferences by dividing the user data according to a spreading ratio, enabling a faster data transmission rate of 11 Mbps. It sets a specific string of bits to be sent for each data bit. A redundant bit pattern is included in the chipping code to increase resistance to interference.

2.2.2.3 OFDM

For 802.11a, OFDM modulation is used instead of the spread spectrum technologies, with the intention of providing less interference. This method supports a high transmission speed of 54 Mbps. It splits a radio signal into multiple smaller sub-signals that are transmitted simultaneously at different frequencies (multi-carrier), thus reducing the amount of crosstalk (electronic interference) during transmission. Task Group 802.11h focuses on improving the spectrum managed in 802.11a-based networks.

2.2.3 MAC Layer

The 802.11 specifications provide asynchronous (DCF) and contention-free (PCF) services. The asynchronous service is always available whereas the contention-free service is optional. DCF implements the basic access method of the 802.11 MAC

protocol; the *carrier senses multiple accesses with collision avoidance* (CSMA/CA) for path sharing. This service was used in our experiments later in the thesis.

The PCF provides contention-free service, which implements a *polling* access method [ANSI/IEEE. Std 802.11, 1999]. It uses a *point coordinator* (PC), usually the AP, which cyclically polls stations, giving them the opportunity to transmit. Thus the access priority provided by a PCF may be utilised to create a *contention-free* access method. The PC controls the frame transmissions of the stations in order to eliminate contention for a limited period of time. Unlike the DCF, the implementation of the PCF is not mandatory. Furthermore, the PCF itself relies on the asynchronous service provided by the DCF (see Figure 2-2).

All physical layers support one common MAC layer. Task Group 802.11e focuses on enhancing the MAC layer for QoS.

2.2.4 Standards and Data Rates

The 802.11 protocols offer two data rate standards, 802.11a and 802.11b, and one work-in-progress data rate standard, 802.11g. Table 2-1 compares the differences among these standards.

Interoperability between different 802.11 vendor products is tested and certified by the Wi-Fi Alliance (formerly the *Wireless Ethernet Compatibility Alliance*, WECA[2]).

2.2.4.1 802.11a

IEEE Std. 802.11a [1999] was built for the wireless *asynchronous transfer mode* (ATM), and operates in the 5 GHz to 6 GHz band. Its OFDM offers a bandwidth of 300 MHz at shorter distances (than 802.11b), and the 802.11 standard defines three types of data rate:

- 6 Mbps using binary phase shift keying for encoding,
- 12 Mbps using quadrature phase shift keying, and
- 24 Mbps using 16-level quadrature amplitude modulation encoding.

[2] See www.wi-fi.org for more information.

However, the de facto standard appears to be 54 Mbps with 64-level quadrature amplitude modulation.

2.2.4.2 802.11b

IEEE Std. 802.11b [1999] is known as Wi-Fi or 802.11 High Rate, providing a 2.4 GHz ISM band with an 11 Mbps data transmission rate. It uses the HR/DSSS and *complementary code keying* (CCK) modulation in order to support higher speed transmission, and is less susceptible to the multipath-propogation interference. 802.11b is backward compatible with 802.11. Its limitations include a bandwidth provision up to 83 MHz, and interference with other wireless technologies, such as microwave ovens, cordless phones, and Bluetooth.

802.11a and 802.11b are compatible with each other, but with different frequencies (5 GHz and 2.4 GHz, respectively). 802.11b is wireless Ethernet while 802.11a is wireless Fast Ethernet.

2.2.4.3 802.11g

Task Group 802.11g [TGg, 2002] is working on extending the 2.4 GHz band for a higher data rate of 20+ Mbps. The 802.11g standard is similar to 802.11b, and is thus backward compatible with it, with an improved transmission rate of 54 Mbps. It uses a combination of OFDM and CCK modulation. Because the radio transceiver uses RF-to-baseband, there is no need for an intermediate frequency.

Characteristics	802.11a	802.11b	802.11g
Frequency Band	5 GHz	2.4 GHz	2.4 GHz
Data Rate (Mbps)	54	11	54
Physical Layer	OFDM	HR/DSSS	OFDM + CCK
Operating Range	Approximately 50 m indoors and 500 m outdoors (Throughput decreases with distance and network load)		
QoS	802.11e patched QoS		
Security	WEP/802.11i proposed mechanisms		

Table 2-1 Comparisons of 802.11 Standards

2.2.5 Communication Exchange

The 802.11 standard specifies nine services to support frame delivery, access control and privacy. These nine services are authentication, association, deauthentication, disassociation, distribution, integration, privacy, reassociation, and frame delivery.

In an infrastructure network, wireless clients and APs must establish a relationship, or an *association*, prior to data communication. Only after an *association* is established can the two wireless stations exchange data. The synchronisation process is a two-step process involving three states:

1. Unauthenticated and unassociated,
2. Authenticated and unassociated, and
3. Authenticated and associated.

The process of a wireless client finding and associating with an AP is shown in Figure 2-5. APs transmit a *beacon* management frame at fixed intervals, containing information such as network names (*service set identifiers*, SSID). To associate with an AP and join an infrastructure BSS, a client listens for beacon messages to identify the APs within range, which is also known as passive scanning. The client then selects a BSS to join. A client may also send a *probe* request management frame to find an access point with a desired SSID, which is known as active scanning.

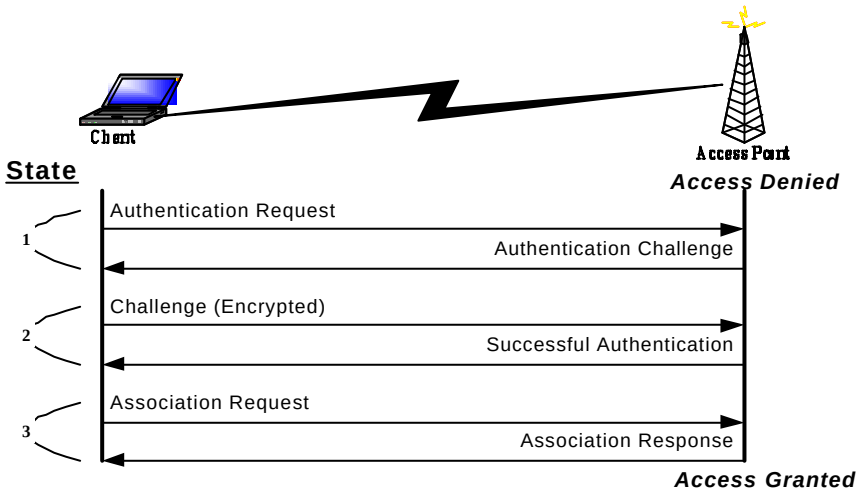

Figure 2-5 Authentication and Association States

After identifying an AP, the client and the AP perform authentication by exchanging several management frames as part of the process. The two standardised authentication mechanisms used are described in Section 3.1.1. After successful authentication, the client moves into the second state, authenticated and unassociated. Moving from the second state to the third and final state, authenticated and associated, involves the client sending an *association* request frame, and the access point responding with an *association* response frame.

2.3 Security

The 802.11 standard provide two types of authentication: *open system* and *shared key* authentication (see Section 3.1.1 for details). The 802.11 standard also specifies an optional privacy method, the WEP protocol, to provide confidentiality for wireless communication.

The open system authentication provides null security protection, while shared key authentication requires using the WEP protocol to provide access control. Details of how these mechanisms operate, and the weaknesses of WEP are discussed in Section 3.2.

2.4 Roaming and Handoff

User mobility supports client stations moving freely from one cell to another. This is also known as roaming. Roaming requires the interaction between APs and DSs. A user can move from cell A to cell B by locating the AP in Cell B, and transferring credentials to that AP to maintain connection without reassociation. This scenario can involve reinitiating a search for an AP, in the same manner the client would when it is initialised, or other means, such as referencing a table built during the previous association [Convery & Miller, 2001]. To provide roaming between cells, APs need to provide effective handoff mechanisms. The 802.11 standard does not stipulate any particular mechanism for roaming; thus, it is up to each vendor to define an algorithm to assist its WLAN clients to make roaming decisions. While this provides greater flexibility in DS and AP functional design, the associated cost is that physical AP devices from different vendors are more likely to have interoperability issues. Roaming between different vendors' APs can result in extended roaming times. Furthermore, how to maintain a user's credential when users move to another cell without breaking the connection, and thus requiring reassociation and reauthentication by the new AP must be considered. Adding to this problem, specific vendor products may have different architectures for handoffs between APs, thus, the user credential handoff between different vendors must be determined.

In the current 802.11 standard, for every frame transmitted, the receiving station responds with an *acknowledgement* (ACK) frame. Client stations use the ACK

messages as a means of determining how far from the access point they have moved. ACK frames and beacons (from APs) provide the client station with a reference point to determine whether a roaming decision needs to be made. If a set number of beacon messages are missed, the client can assume that it has roamed out of range of the access point with which it is currently associated. In addition, if expected ACK messages are not received, clients can also make the same assumption.

The 802.11 workgroup [IEEE 802.11 WG, 2002] has recognised this problem by stating, "this limitation has become an impediment to WLAN market growth". Task Group 802.11f [IEEE Std. 802.11/D3.1, 2002] has been set up to develop recommended practices for an *inter-access point protocol* (IAPP) that provides the necessary capabilities to achieve multi-vendor AP interoperability across a DS supporting 802.11 WLAN connections. This recommended practice specifies the information to be exchanged between APs, as well as with higher layer management entities (such as *remote access dial-in user service* [RADIUS] protocol) to support the 802.11 DS functions based on the *internet protocol* (IP). Mobile IP provides the capability for supporting uninterrupted IP network connectivity when users roam. Lee [2002] examined several alternatives of Mobile IP and AAA integration to provide user roaming.

Roaming and handoff are important issues in WLANs; however, the scope of this thesis is limited to a single cell design.

2.5 Summary

This chapter has presented an overview of different types of wireless technologies such as cellular networks, 802.11, and Bluetooth. Discussion in the chapter concentrated on the 802.11 WLAN architecture, which is the protocol used in the experiments (802.11b) for this study. Architectures, physical and MAC layers, data rates, and the communication exchange of the 802.11 standard were examined. Roaming considerations for WLANs were discussed, and it was noted that this research conducted only a single cell design testbed.

CHAPTER 3

WLAN Security Technologies

Wireless LANs have gained increasing market popularity in locations such as airports, cafés, universities, and businesses, but WLAN security remains an ongoing concern. The rapid deployment of WLANs has further emphasised the security vulnerabilities in the 802.11 standard. The original 802.11 standard specified only security provisions sufficient for wired networks; end-to-end security cannot be ensured.

In this chapter, we investigate existing and proposed WLAN security technologies to improve the 802.11 standard. Security concerns over WLAN vulnerabilities are explored, and associated techniques are provided to mitigate these vulnerabilities. We also analyse the two types of AAA integrated network security solutions, 802.1X and VPNs.

3.1 Security of the IEEE 802.11 Standard

In this section, we examine the security mechanisms provided by the 802.11 standard. Vulnerabilities such as weak key derivation and management have been identified in the WEP protocol. Improvements in key management and authentication to fix these flaws are presented.

3.1.1 802.11b Security Mechanisms

The 802.11 standard provides two types of authentication (open system and shared key), and a privacy method (WEP), as shown in Table 3-1. These mechanisms mainly deal with the security provisions in the link and physical layers of the *open systems interconnection* (OSI) model. They do not support either end-to-end or user-authentication. The standard only aims to make wireless networks as secure as its wired counterparts.

Authentication Method	Open System and Shared Key
Privacy Method	WEP (optional; to be used with Shared Key)

Table 3-1 802.11 Authentication and Privacy Methods

3.1.1.1 Authentication

- Open System Authentication

  This is the default authentication service. It is in fact 'null' authentication, i.e. no authentication at all and this method authenticates any clients who request to join a network.

- Shared Key Authentication

The same secret (thus global) key is shared between an AP and stations to authenticate stations joining a network. The key resides in each station's *management information base* (MIB) in write-only form and is available only to the MAC layer. This method requires the use of the WEP mechanism.

The process of the shared key authentication operates in four steps:

- The requesting station sends an authentication frame to the AP.
- The AP receives the authentication frame and replies with a random challenge text generated by the WEP encryption engine, using the *pseudorandom number generator* (PRNG).
- The requesting station copies the challenge text in an authentication frame, then encrypts it with the shared secret key. The encrypted frame is sent back to the AP.
- The receiving AP decrypts the text with the same shared key, and compares it to the challenge text sent earlier. Confirmation is sent if a match occurs, else a negative authentication is generated.

3.1.1.2 Privacy

The 802.11 standard includes the WEP as an optional protocol. WEP ensures the confidentiality and integrity of data transmitted between users when using shared key authentication.

3.1.1.2.1 WEP Protocol

WEP encryption uses the same 60-bit shared secret key to encrypt and decrypt data. In WEP, it is necessary to generate a different *Rivest Cipher 4* (RC4) key for each packet from a shared key. WEP was not designed for high security, but rather to be at least as secure as its wired counterpart. Two processes work inside the algorithm; one encrypts the plain text while the other protects the data's integrity. The main components of this algorithm use an *initialisation vector* (IV) of 24 bits, PRNG and

an *integrity check value* (ICV) of 32 bits, as shown in Figure 3-1. The secret key is concatenated with an IV and the resulting *seed* is input to a PRNG.

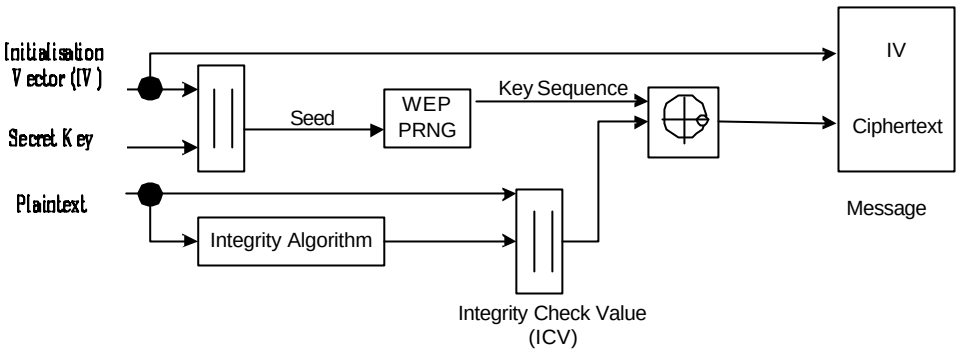

Figure 3-1 WEP Encipherment Block Diagram [ANSI/IEEE. Std 802.11, 1999]

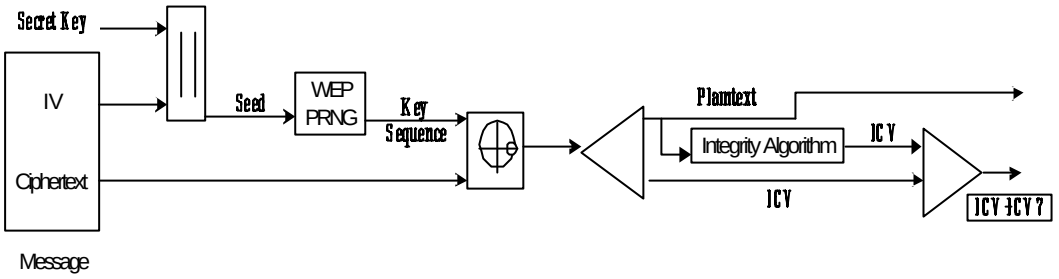

Figure 3-2 WEP Decipherment Block Diagram[ANSI/IEEE. Std 802.11, 1999]

A frame contains the encrypted data (ciphertext block) together with the ICV and the cleartext IV (Figures 3-1 and 3-2). Data integrity is provided by the ICV. The output message is generated by concatenating IV and the secret key (the key remains constant), while the IV changes periodically when connections between devices are made [Weatherspoon, 2000]. The IV can be reused after a limited time; this is one of the major weaknesses of WEP (see Section 3.1.2), because the standard specifies a very weak key derivation and management. The keys generated for different data packets are too similar because the IV is very limited. Furthermore, static key management of WEP requires manual configurations on wireless devices, thus, as the numbers of clients grow, administration overheads increase.

Vendors have provided support for a stronger WEP key length of 128-bits in their WLAN solutions. However, this method is still vulnerable to attacks, as we explain in the next section.

3.1.2 WEP Safety Issues

In many reported incidents, attacks on WLANs showed that WEP was not activated [Held, 2001; WECA, 2001a]. Vendors provide a deactivated WEP as a default installation, but a survey conducted by Gartner found that about "60 percent of Wi-Fi (802.11b) installations did not even turn the WEP on" [McDonough, 2002].

The WEP in the 802.11 standard provides only limited support in safeguarding the network. The vulnerabilities in WEP's cryptography design have led to security problems such as modification of data, redirection attacks, rogue APs, and replay attacks.

Borisov et al. [2001] discovered that the WEP has fundamental flaws in the cryptographic design of the implementation of the RC4 encryption algorithm and checksum methods. In particular, this relates to key reuse and weak message authentication. They claimed that the WEP's goals of securing confidentiality, access control, and data integrity had all failed. The classical 40-bit and extended versions of the 128-bit key size provided by the WEP did not deter hackers, indicating that key size was irrelevant. The 24-bit IV is prone to reuse frequency, because the vector size is limited. IV collisions produce identical WEP keys when the same IV is used with the same shared secret key for more than one data frame, and this is the weakness that attackers exploit. This claim is supported by an early study by Walker [2000], which showed that regardless of key size, the vulnerability in RC4 prevented the WEP from providing "a meaningful notion of privacy to users". In addition, weak message authentication made it possible to inject traffic into the network. Although long key-length versions of WEP were released to the market, the flaws in WEP were not caused by a shorter key.

An experiment on the security mechanisms mentioned previously was conducted by Arbaugh et al. [2001]; they discovered weaknesses in the 802.11 access control mechanism even when it was used with the WEP authentication method. Thus they stated, "all of these (even vendors' proprietary security) mechanisms are completely ineffective". This weakness increases the risk of rogue AP networks and station redirection attacks (see Section 3.2).

Considering these three papers, all the security mechanisms in 802.11 are compromised. Until this point, attacks on the WEP were based on the design of the system, and users assumed the underlying cryptography, RSA[3]'s RC4 algorithm, was sound. Fluhrer et al. [2001] presented the final blow to WEP security when they found "weaknesses in the key scheduling algorithm" of RC4. These flaws made the RC4 keys fundamentally weak, and the authors designed an attack that would allow a passive user to recover the secret WEP key simply by collecting a sufficient number of frames encrypted with weak keys. An implementation of the attack was carried out by Stubblefield et al. [2001]. Tools to plan an attack (such as AirSnort and WEPCrack) exist, and key recovery with AirSnort takes only a few seconds when a sufficient number of weakly encrypted frames are gathered.

These studies showed that the WEP security mechanism is ineffective unless good key management is designed. The vulnerabilities in 802.11 can be generalised as follows:

- No dynamically generated session keys
- Static WEP keys
- No mutual authentication

3.1.3 WEP Improvements

The link layer security provisions in the 802.11 standards are all vulnerable to attacks. Therefore, systems should deploy "additional higher-level security mechanisms such as access control, end-to-end encryption, password protection, authentication, virtual private networks, or firewalls" [WECA, 2001a] and assume WEP as a very basic layer of security only.

The IEEE 802.11 committee has set up task group 802.11i [TGi, 2002] to enhance the security and authentication mechanism of the current 802.11 MAC. Their work has resulted in the development of:

- Replacement of the 802.11 standard with 802.1X authentication and key management.

[3] Rivest Shamir and Aldeman, an IT company providing security mechanism and products, see www.rsa.com.

- Improvement of the exiting WEP with *temporal key integrity protocol* (TKIP), also known as WEP2.
- Deployment of *enhanced security network* (ESN) solution with a stronger encryption algorithm.

3.1.3.1 Replace 802.11 Authentication & Key Management with 802.1X

The 802.1X standard has been introduced to provide a centralised authentication and dynamic key distribution for 802.11 architecture utilising the 802.1X standard with RADIUS [Roshan, 2001; Task Group i, 2002]. 802.1X is an authentication standard for 802-based LANs using port-based network access control. The 802.1X standard is used for communication between wireless clients and APs, while RADIUS operates between an AP and an authentication server (see Section 3.5).

3.1.3.2 Improve WEP with TKIP

The TKIP solution deploys a hashing technique that generates a temporal key (a unique RC4 key) to derive a per data packet key. This strengthens the RC4 key-scheduling algorithm by pre-processing the key and the IV by passing them through hashing.

The solution consists of:

- An encryptor and decryptor that share a RC4 104-bit or 128-bit secret key. This key is called the *temporal key* (TK).
- An encryptor and decryptor that use the RC4 stream cipher.
- An IV value that is not used more than once with each TK. Implementations must ensure that the TK is updated before the full 16-bit IV [Housley & Whiting, 2001] or 48-bit IV [Housley et al., 2002] space is exhausted. The 48-bit IV solution provides a longer key life span than 16-bit IV.

The solution specifies a two-phase processing of the TK to determine the per-packet encryption key. *Phase one* involves key mixing where the *transmitter address* (TA) is mixed into the TK to ensure that the various parties encrypting with the TK use different key streams. By mixing the TA and the TK, a different set of keys is used by each party. Traffic sent by a STA to the AP will use a different set of keys than traffic sent by the AP to the STA. This output is likely to be cached to improve performance

and can be reused to process subsequent packets associated with the same TK and TA. *Phase two* mixes the output of the first phase with the IV and generates a unique per-packet key for each data packet. To avoid any repetition of keys, the IV must be different for each packet encrypted under the TK.

3.1.3.3 Deploy ESN Solution

The ESN solution is focused on stronger encryption for data over wireless networks by using a non-proprietary 128-bit encryption solution, which will support the *advanced encryption standard* (AES) encryption algorithm. Also, HMAC[4]-SHA1-128 can be used as the hashing function to support message authentication with AES [TGi, 2002].

3.2 Wireless Security Threats and Risks

Wired and wireless LANs share some common security risks: physical security, insider attacks, unauthorised access and eavesdropping. A study published by the Wi-Fi Alliance in October 2001 found that "security has been, and remains, the overriding concern regarding wireless networking deployment" [WECA, 2001b], among 72% of wireless intenders and 50% of wireless adopters.

3.2.1 Types of Security Threats

A taxonomy of security threats is depicted in Figure 3-3. These attacks can come from internal or external sources.

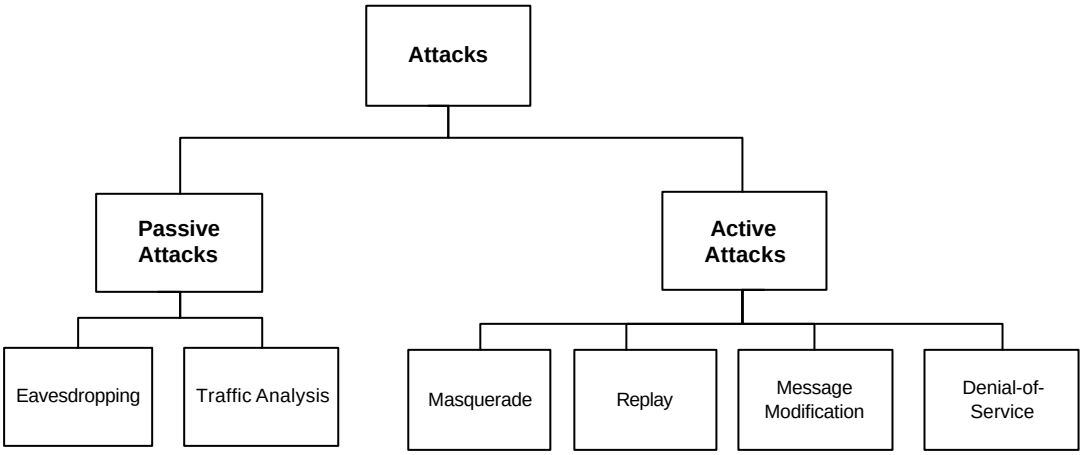

Figure 3-3 Taxonomy of Security Threats [Karygiannis & Owens, 2002]

[4] *Hashed message authentication code* (HMAC) with either *message digest algorithm* (MD5) or *secure hashing algorithm* (SHA1).

3.2.1.1 Passive Attacks

An unauthorised party gains access to a network and does not modify the resources on the network. Types of passive attack include:

- *Eavesdropping:* An attacker simply monitors and listens to message content transmissions. For example, an unauthorised person drives through the city and listens to various WLAN transmissions within different organisations (i.e. war driving, see Section 3.2.3 for more details).
- *Traffic Analysis:* An attacker monitors the traffic for communication pattern analysis. The statistics collected can be used to perform a dictionary attack.

3.2.1.2 Active Attacks

An unauthorised party gains access to a network and modifies the resources on the network. An attacker must first spoof either the MAC address and/or IP address of a user/device to gain network access, and then change the content of the network resources. Types of attack include:

- *Masquerading:* An attacker impersonates an authorised user and thereby gains certain unauthorised privileges. Masquerading includes the use of spoofing, rogue APs, and redirection attacks. An attacker can fool users to log in to the rogue AP by placing a rogue AP in the same area as a valid AP, sending the same SSID but with a stronger signal than the valid AP. The attacker is able to decipher the shared key from the traffic collected. The rogue AP can be used to redirect users' transmissions to an invalid destination, or to insert deauthentication packets.
- *Replay:* An attacker monitors the traffic (passive attack) then retransmits the message as the legitimate user.
- *Message Modification:* An attacker alters the legitimate message by deleting, adding, changing, or recording it. Furthermore, an attacker may wish to alter the configuration of a device, using, for example, *simple network management protocol* (SNMP) to configure APs.
- *Denial-of-service* (DoS): An attacker prevents or renders the normal use or management of network systems useless by issuing malicious commands or injecting a large amount of traffic that fills up the radio

frequency. This type of attack can be further extended to *distributed DoS (DDoS)* attacks.

3.2.2 Physical Security of Wireless Devices

Physical security is the most fundamental step in ensuring that only authorised users have access to wireless devices such as laptops, handhelds, and APs. APs (or base stations) must be difficult to access to prevent security breaches, and the AP must be placed for an adequate coverage area. For example, the improper placement of an AP might allow an attacker to bypass other security measures, such as modifying the AP configuration by direct connection. Physical locks, cipher locks, and biometric systems can be used to counter thefts.

3.2.3 WLAN Attacks

Wireless networks without proper security implementation can be penetrated easily. The physical freedom of a WLAN is also its vulnerability; traffic is no longer confined to a wire. Privacy concerns over data transmission increase because data on a WLAN is "broadcast for all to hear" [O'Hara & Petrick, 1999]; eavesdropping becomes easy. In addition, RF-based networks are open to packet interception by any receiver within range of a data transmitter. 802.11 beacon frames, used to broadcast network parameters, are sent unencrypted. Thus by monitoring beacon frames, wandering users with an 802.11 receiver can discover wireless networks in the area.

In addition, the deployment of wireless networks opens a "back door" [Arbaugh et al., 2001] into the internal network that permits an attacker access beyond the physical security perimeter of the organisation. The lack of a physical boundary allows attacks such as sniffing, resource stealing, traffic redirection, DoS, SSID, and MAC address masquerading to occur.

War driving is similar to *war dialling* (dialling every number looking for a modem backdoor into a network), and the Wall Street Journal reported an incident in which two people armed with wireless tools were able to drive around Silicon Valley and intercept traffic such as emails over unprotected WLANs [Bansal, 2001]. Another example was an audit carried out of four major airports in the US [Brewin & Verton, 2002]. This study found that WLANs in applications such as passenger check-in and

baggage transfers were operating without even some of the most basic forms of security protection. Using NetStumbler, an AP-detection tool, the authors discovered that only 32 of the 112 WLAN APs had the WEP protocol turned on, and most of the APs were broadcasting plaintext SSIDs. Furthermore, the authors detected several WLAN APs operating at Chicago's International Airport with broadcast SSIDs of "X-ray" and unencrypted files were transmitted.

Other new types of attacks include *warspammers* and *warchalking*. Warspamming takes advantage of unprotected WLANs to bombard email users with unsolicited and unwelcome messages. Warchalking takes place when hackers draw a chalk symbol on a wall or piece of pavement to indicate the presence of a wireless networking node. Warchalking was originally developed to alert system administrators to their wireless network security lapses [Wearden, 2002].

3.3 Risk Mitigation and Countermeasures

WLAN risks can be mitigated by applying both basic and AAA infrastructure countermeasures to address specific attacks and threats. Basic countermeasures involve altering the existing security functions provided within wireless equipment. These countermeasures provide only limited defence against casual attacks; for determined adversaries, organisations should consider AAA integrated solutions. The AAA infrastructure countermeasures provide integrated solutions using existing AAA infrastructure components such as the RADIUS protocol (see Section 3.4) and *public key infrastructure* (PKI, see Section 3.7), with network solutions such as VPN and the 802.1X standards.

3.3.1 Basic Countermeasures

Every wireless device comes with different default settings; such built-in configurations can be prone to security vulnerabilities. This section discusses basic security protection to prevent casual attacks.

3.3.1.1 Change Default Password

Default passwords such as "public" or blank passwords are not sufficient protection. Administrators should deploy strong passwords of at least 8 characters that are

consistent with the organisation's security policies. When combining this with AAA infrastructure solutions, two-factor authentication can be implemented.

3.3.1.2 Change SSID

The factory default SSID for an AP may provide network names like "Tsunami", which can easily be detected. The SSID should not provide information on the function or location of an AP such as X-ray. Naming convention of SSIDs should be formed according to an organisation's policy, an example is shown in Figure 3-4 (adapted from Gast [2002]).

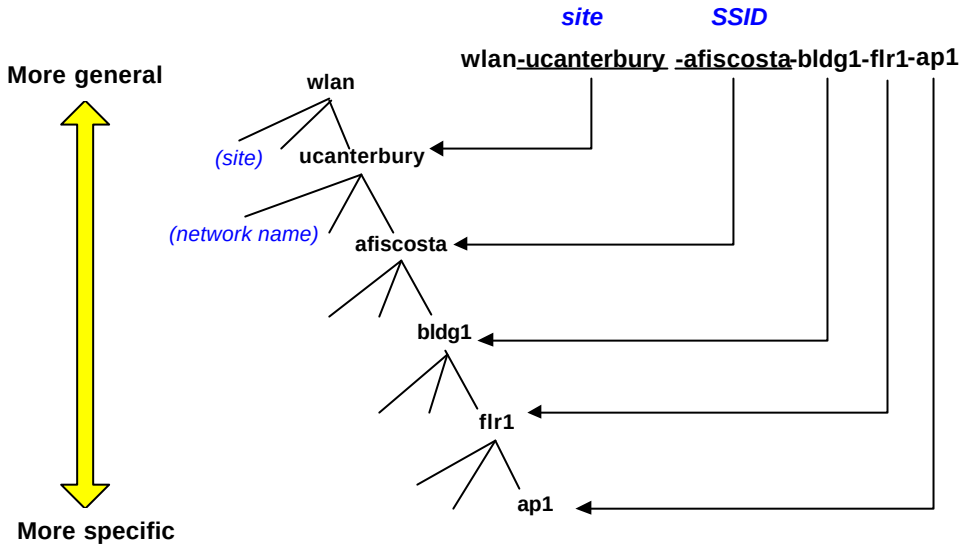

Figure 3-4 An Example of Naming Conventions for Wireless Devices

3.3.1.3 Enable MAC Authentication

A MAC address is a hardware address that uniquely identifies each device on a network (e.g. a wireless network adapter). They identify devices, not users. Vendors[5] provide MAC-address filtering capability to regulate communication among different computers on a network. During the initial connection procedures, wireless APs can check the MAC address of connecting stations to ensure the station is on the list of known good MAC addresses, called a MAC *access control list* (ACL). However, a MAC ACL does not provide strong authentication against determined attacks. MAC addresses are transmitted in cleartext from a wireless *network interface card* (NIC) to an AP; eavesdropping software can easily capture MAC addresses. Furthermore, users

[5] For larger organisations with multiple APs, consider storing the MAC list at a centralised location using a RADIUS server.

with sufficient operating system privileges can alter addresses to masquerade as an allowed wireless-network user.

Address filtering relies on *information technology* (IT) departments issuing wireless LAN cards to users and maintaining an organisation-wide list of MAC addresses allowed to connect to a wireless network. This might be impractical in medium-to-large organisations because it increases the administrative burden.

3.3.1.4 Protect the AP Placement

Improper placement of APs (Section 3.2.2) can lead to security breaches. If malicious users can gain physical access to an AP, they would be able to change the configuration of the AP. Organisations need physical security on their wireless devices. Regular security audits ensure risk mitigation.

3.3.1.5 Enable WEP Authentication

Built-in security configurations do not enable the WEP security function by default. To provide at least some basic defence against attacks, shared authentication should be used instead of open system authentication.

3.3.1.6 WEP Encryption

Deploy the strongest encryption method available whenever possible. The shared secret key value provided as the default setting must be changed to prevent security breaches. Note that enabling the WEP mechanism can only prevent basic attacks (Section 3.2.3), and for determined adversaries, the WEP key length is unsafe at any size (Section 3.1.2).

3.3.1.7 Change SNMP Parameters

SNMP agents can be configured in APs to allow network management software tools to monitor the status of an AP and its clients. The default SNMP community string commonly used by SNMP agents is the word “public” with assigned “read” or “read and write” privileges. To prevent unauthorised users from writing data to an AP (an integrity breach), SNMP parameter settings must be changed or disabled (if SNMP is not required in the organisation).

Several vendors use SNMP as an AP management mechanism and thereby increase vulnerabilities. For example, one vendor uses SNMPv1 for AP management, thus all management traffic traverses the network unencrypted. Another vendor allows SNMP read access to WEP keys, even though WEP keys must remain secret. Most vendors use cleartext telnet for remote command-line interfaces. Web-based interfaces are nearly all simple HTTP and do not use *secure socket layer* (SSL) or *transport layer security* (TLS) for protection.

Improvements for network resource management may consider using SNMPv3 or *policy based network management* (PBNM, [Wong, 2001]) with *common open policy service* (COPS) protocol for better security.

3.3.1.8 Change the Default Channel

To prevent DoS attacks and radio interferences between two or more APs in close location, the channel setting of an AP must be changed to operate in a different frequency band.

3.3.1.9 DHCP Usage

Automatic network connections involve the use of a *dynamic host control protocol* (DHCP) server. The DHCP automatically assigns IP addresses to clients that associate with an AP. Using DHCP allows users the advantages of roaming or establishing ad hoc networks. However, the threat with DHCP is that a malicious user can easily gain unauthorised access using a mobile device, because DHCP may not know which wireless access devices have access permission, and might automatically assign the device a valid IP address. Depending on the size of the network, disabling DHCP and using static IP addresses may be feasible.

A solution to overcome DHCP threats might involve placing the DHCP behind the wired network's firewall, which grants access to a wireless network located outside the firewall. If user authentication and access control are moved to the link layer, then threats to the DHCP are limited to insider attacks. An AAA integrated solution such as 802.1X authentication can mitigate DHCP risk.

3.3.2 AAA Infrastructure Solutions

AAA infrastructure provides centralised network management. Several AAA protocols exist, such as RADIUS (see Section 3.4 for more detail). Existing network solutions such as VPNs incorporate AAA infrastructure; and it is essential to provide remote access control for dial-in users. Enhancing WLAN security requires integration with an AAA infrastructure to overcome security vulnerabilities. Two security solutions have been recommended in various studies [Borisov et al., 2001; Caballero & Malmkvist, 2002; Convery & Miller, 2001; Karygiannis & Owens, 2002; TGi, 2002]:

- 802.1X Solution
- VPN Solution

3.3.2.1 802.1X Solution

This solution utilises the existing 802.1X standard, incorporating the port-based network access control for 802.11 infrastructures, and leveraging AAA protocols to support wireless LAN security. Authentication methods are based on an *extensible authentication protocol* (EAP) to provide integration capability (with future authentication methods[6], see Section 3.5).

3.3.2.2 VPN Solution

This solution applies the existing wired network solution to the wireless counterparts, using security mechanisms such as *IP Security* (IPSec) and tunnelling (see Section 3.6).

3.3.3 Additional Enhancements

Additional enhancements can be applied regardless of whether or not an integrated network security solution exists in the organisation.

3.3.3.1 Firewalls

Placing a firewall between the trusted wired network and untrusted wireless networks provides an extra layer of access control [Harris, 1998]. Interoperability between

[6] This group includes *secure remote password* (SRP) and *tunnelled transport layer security* (TTLS) authentication methods, but they have not been widely adopted yet, but may become future mainstream authentication choices.

vendors' products must be considered when a firewall facilitates the traffic flow between wired and wireless networks.

Implementing personal firewall software on client computers can provide some protection against attacks, especially for clients accessing public WLANs. Organisations can set up these personal firewalls to be centrally or user managed.

3.3.3.2 IDS

An *intrusion detection system* (IDS) provides effective security against unauthorised attempts to alter network resources, whether the network has been compromised or accessed. It minimises the risk of an intruder breaking into authentication servers and compromising databases. Some IDS systems are specially designed for the WLAN environment, such as AirDefense IDS.

3.3.3.3 Anti-Virus Software

In common with wired networks, anti-virus systems provide another level of security against attacks, such as virus, worms and Trojans. Organisations should deploy anti-virus software on both authentication servers and wireless clients to ensure system integrity.

3.3.3.4 Software Upgrades and Patches

Regular updates on software patches and upgrades, such as AP management software, will assist in ensuring that as many security vulnerabilities have been identified and corrected as possible.

3.3.3.5 Application Layer Security

Additional access control can by provided using applications with strong built-in cryptographic systems. In particular web-based systems can be secured with the SSL or TLS and host logins can be secured with *secure shell* (SSH[7]). Other environments may have already deployed a framework such as Kerberos for application layer security, which may be able to be configured for wireless networks (e.g. Windows 2000-based networks).

[7] Also known as secure socket shell.

3.4 AAA Infrastructure

AAA [Mitton et al., 2001] is important in both wired and wireless networks to ensure network security as well as providing a mechanism for billing. AAA protocols currently include RADIUS, *terminal access controller access control system* (TACACS, [Finseth, 1993]), and DIAMETER. RADIUS and TACACS were developed for remote user dial-in services and were not specifically designed to support wireless access networks. TACACS is a Cisco proprietary products and an improved version is called TACACS+.

DIAMETER [Calhoun et al., 2002] in contrast, takes wireless network access into consideration and supports applications such as IP mobility and roaming. RADIUS is the most widely deployed protocol for services such as dialup *point-to-point protocol* (PPP) and terminal server access. Infrastructure networks often deploy AAA architecture to ensure network access control (examples include VPN solutions). In this thesis, RADIUS is the AAA protocol used to deploy WLAN security solutions. Furthermore, this study concentrated on the interaction between authentication and encryption, accounting methods and usage were outside our scope.

3.4.1 RADIUS

RADIUS is defined in RFC 2865 [Rigney, Willats, Rubens et al., 2000] and RFC 2869 [Rigney, Willats, & Calhoun, 2000], and is used in a client/server environment (Figure 3-5), and has been widely used by businesses and *Internet service providers* (ISPs) to control remote access.

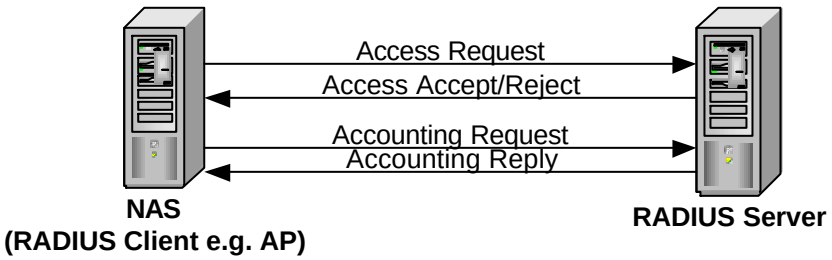

Figure 3-5 RADIUS Communication Exchange

A RADIUS client is a type of *network access server* (NAS), and sends authentication and accounting requests to the RADIUS server in order to gain network access.

RADIUS servers are responsible for authenticating users' requests from a NAS and grant or reject access based on user credentials. RADIUS accounting is used to collect accounting data on users for billing, auditing, or trend analysis purposes. Interactions between the client and RADIUS server are authenticated through a shared secret that is never transmitted over the network. UDP (rather than TCP) is used as the transport protocol for RADIUS (port 1812 for authentication and port 1813 for accounting). RADIUS supports a variety of authentication methods, including EAP. AAA servers based on the RADIUS protocol include Microsoft's Internet Authentication Server (IAS), Cisco's Access Control Server (ACS), and FreeRADIUS. Microsoft IAS was the RADIUS server used in this study. Caballero and Malmkvist [2002] investigated and designed a NAS using the RADIUS protocol for public WLAN access networks, while Lee [2002] evaluated different interactions of AAA architecture with mobile IP for WLANs.

3.4.1.2 Authentication Protocols

An AAA server can support different types of user authentication methods:

- *Password authentication protocol* (PAP) uses cleartext passwords. It provides low security protection against unauthorised access.
- *Challenge handshake authentication protocol* (CHAP) is a challenge-response authentication protocol using an industry-standard *message hashing5* (MD5) one-way encryption scheme to encrypt the response[8].
- Microsoft-CHAP (MS-CHAP) is a proprietary protocol that supports one-way, encrypted password authentication. If the AAA server supports MS-CHAP, data encryption can be carried out using *Microsoft point-to-point encryption* (MPPE), which is based on the RC4 algorithm. MS-CHAP2 is an improved version and offers mutual authentication.
- *Shiva Password Authentication Protocol* (SPAP) is a two-way reversible encryption mechanism employed by Shiva.
- EAP protocol defined in RFC 2284 [Blunk & Vollbrecht, 1998], is a general protocol for PPP authentication that supports multiple authentication mechanisms. EAP does not select a specific authentication mechanism at the link control phase, but rather postpones

[8] In a Microsoft environment, users' passwords need to be stored in reversible encrypted format.

this until the authentication phase. The client and AAA server negotiate the exact authentication method to be used (see Section 3.5.2 for more detail). EAP supports the following authentication types:

- ✓ MD5-CHAP encrypts user names and passwords with an MD5 algorithm. This is equivalent to CHAP.
- ✓ TLS uses digital certificates or smartcard devices. Authentication requires a user certificate and private key.
- ✓ Additional support for third-party authentication such as *tunnelled TLS* (TTLS) from Funk.

3.5 IEEE 802.1X Standard

The 802.11 working group has adopted the IEEE 802.1X standard, providing *port based network access control*, a mechanism that uses the physical access characteristics of the IEEE 802.LAN infrastructure. The 802.11 TGi has taken the IEEE Std. 802.1X [2001] as its base to control network access on point-to-point connections, and adds several features for 802.11 LANs (WLANs). These features include dynamic key management and user-based authentication (whereas WEP only provides device-based authentication).

Leveraging open standards such as EAP [Blunk & Vollbrecht, 1998], and RADIUS, the 802.1X standard (Figure 3-6, adapted from Orinoco [2002]) enables interoperable user identification and centralised management. Mutual authentication (e.g. TLS) can be carried out to ensure that the derived keys arrive at the right entity, avoiding attacks from rogue APs. Two communication protocols are used to facilitate the 802.1X exchange. Together they form the underlying EAP framework (see Section 3.5.1 for more details):

- EAP over LAN (EAPOL) is used between the authenticator's *port access entity* (PAE) and supplicant's PAE,
- EAP over Wireless (EAPOW) is another EAPOL packet type defined for use in transporting global keys (EAPOW-keys),
- EAP over RADIUS (de-facto), the authenticator PAE communicates with the *authentication server* (AS) using the EAP protocol carried in a higher layer protocol, such as RADIUS.

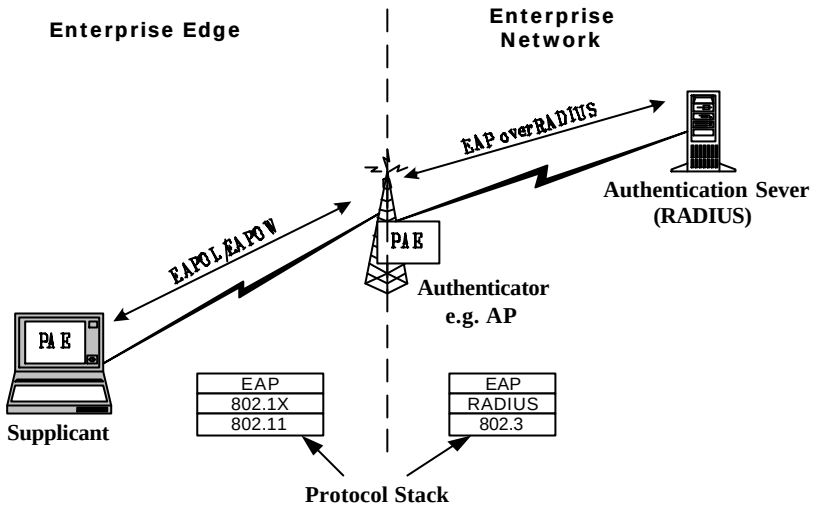

Figure 3-6 802.1X over 802.11 Topology

Key management provides the ability for an AP to distribute or obtain global[9] key information to/from attached stations, through the use of the EAPOL-key messages, after successful authentication. EAPOL defines the encapsulation techniques used in order to carry EAP packets between the client and an AP. Note that 802.1X authentication occurs after 802.11 associations (see Section 2.2.5). Keys are derived on the client and the AAA server (in this case the RADIUS server).

If negotiation of a session key during authentication is required, the use of EAP-TLS protocol is recommended. Thus, 802.1X can derive keys that provide per session key authentication, integrity, and confidentiality. However, it does not provide these per se, but only assists in deriving keys for the session; cryptographic support from WEP, *triple data encryption standard* (3DES), or AES is required to provide encryption. 802.1X requires an authentication protocol and EAP-TLS (RFC 2246, [Dierks & Allen, 1999]) is commonly used to support the key derivation algorithm.

3.5.1 802.1X Architecture

The standard defines the following components, shown in Figure 3-7 (adapted from IEEE 802.1X standard). The architecture can be used with any 802 networks, such as 802.3 and 802.11. At the top of the diagram, we illustrate the physical components above the logical model that may be used for a WLAN environment.

[9] Global key are the same shared keys for every client; these are also called multicast keys.

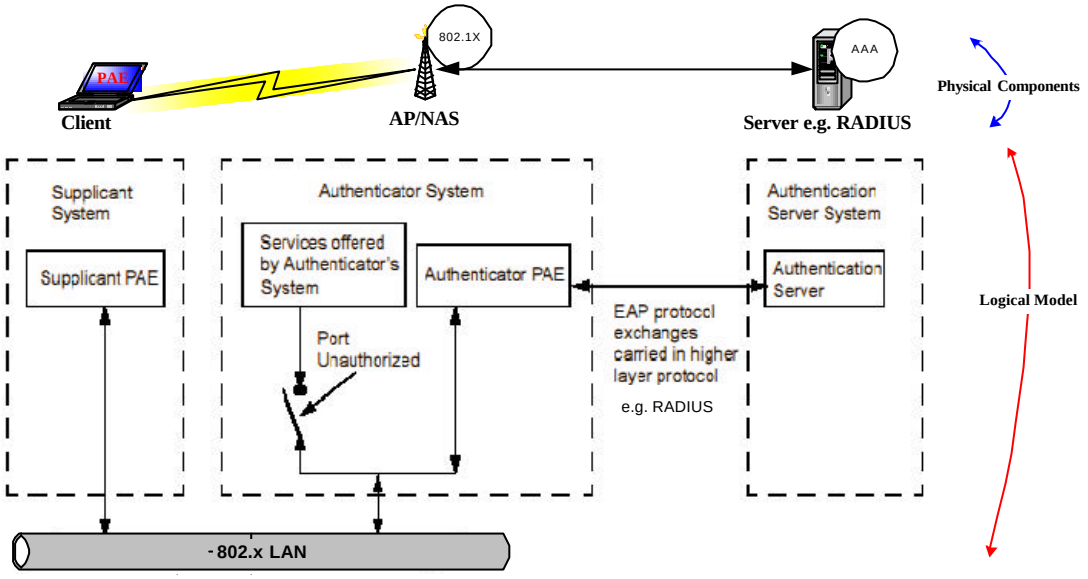

Figure 3-7 802.1X Architecture

- Port

This is a single point of attachment to the LAN infrastructure. It may be a physical network interface or a virtual MAC such as the *logical* ports managed by an AP in an 802.11 LAN.

- PAE

The protocol entity associated with a port. It can support the protocol functionality associated with either the authenticator, the supplicant, or both.

- Supplicant

A component at one end of a point-to-point LAN segment and is authenticated by an authenticator attached to the other end of that link. Supplicants are also called client stations in our research.

- Authenticator

The authenticator is at the other end of the LAN segment and facilitates authentication of the component attached to the other end of that link. It is important to note that the authenticator's functionality is independent of the actual authentication method. It simply acts as a pass-through for the authentication server.

- AS

This is a component that provides an authentication service to an authenticator. It determines whether a supplicant is authorised to access the services by the authenticator based on the supplicant's credentials.

It is possible to authenticate using just the AP only, although in practice all authentication should be carried out by the AS. It is more desirable to implement an AAA server (in this case a RADIUS server) to centrally manage access control. In such situations, the authenticator is expected to act as an AAA client.

3.5.2 EAP

An EAP authentication protocol allows greater flexibility and scalability for future authentication support without the need to change the AP or the NIC. Authentication and key exchange can be upgraded without hardware modifications, avoiding limitations commonly associated with the WEP.

Authentication processes can be performed using a username/password combination or digital certificate. A certificate is similar to a passport, and is issued by a trusted authority (see Section 3.7 PKI) to provide a strong one-to-one relationship. Furthermore, EAP authentication methods can support encryption key generation to protect the information transferred between the supplicant and the AS. Major types of EAP include:

- *EAP-MD5* is equivalent to CHAP [Simpson, 1996]. The client is authenticated by the AS using the password supplied by the client. No mutual authentication can be performed, as the client cannot authenticate the AS. There are no encryption keys generated during the authentication process.
- *EAP-TLS* [Aboba & Simon, 1999] provides mutual authentication of the client and the AS, and is carried out using digital certificates. The AS requires access to the certificate repository, and encryption keys are generated during the exchange. Certificates may be replaced by smartcards; Windows 2000 platform supports such an authentication process [Aboba & Simon, 1999].
- *EAP-Tunnelled TLS (TTLS)* is a Funk proprietary [Funk & Blake-Wilson, 2002; Orinoco, 2002] authentication mechanism. It combines EAP-TLS and traditional password-based methods [Orinoco, 2002] such as CHAP, and *one time passwords* (OTP). The client does not need a digital certificate, but can be authenticated using a password. The client authenticates the server via an X.509 certificate, while the server

authenticates the client by its encrypted password. Encryption keys are generated during the exchange.

- *EAP-SRP* assumes that both the client and the AS are authenticated using a password supplied by the client [Orinoco, 2002; Wu, 2000]. Clients are not required to store or manage any long-term keys, which eliminate the reusable password problem. Encryption keys are generated during the exchange.

EAP-TLS and EAP-MD5 protocols are the common authentication methods associated with 802.1X deployments. This thesis is limited to analysis of both of these methods.

3.5.3 802.1X over 802.11

Applying the 802.1X structure to the 802.11 network architecture (Figure 3-8) provides a controlled wireless network with user identification, centralised authentication, and key management. Dynamic key management in an 802.1X framework rectifies the drawbacks in the WEP security mechanism by deploying per-user session keys.

802.1X authentication is carried out after an 802.11 association. Prior to authentication, the AP filters all non-802.1X traffic to and from the client. Only after the AS has successfully authenticated the client, can it be allowed to access the network. The IETF Network Working Group has presented a draft on 802.1X RADIUS usage [Congdon et al., 2002], supporting a RADIUS server as the backend AS. Keys derived between the client and the RADIUS server are transferred from the RADIUS server to the AP after successful authentication. The secret shared between the RADIUS server and its client will be used to encrypt the attribute containing the keys, in order to avoid eavesdropping.

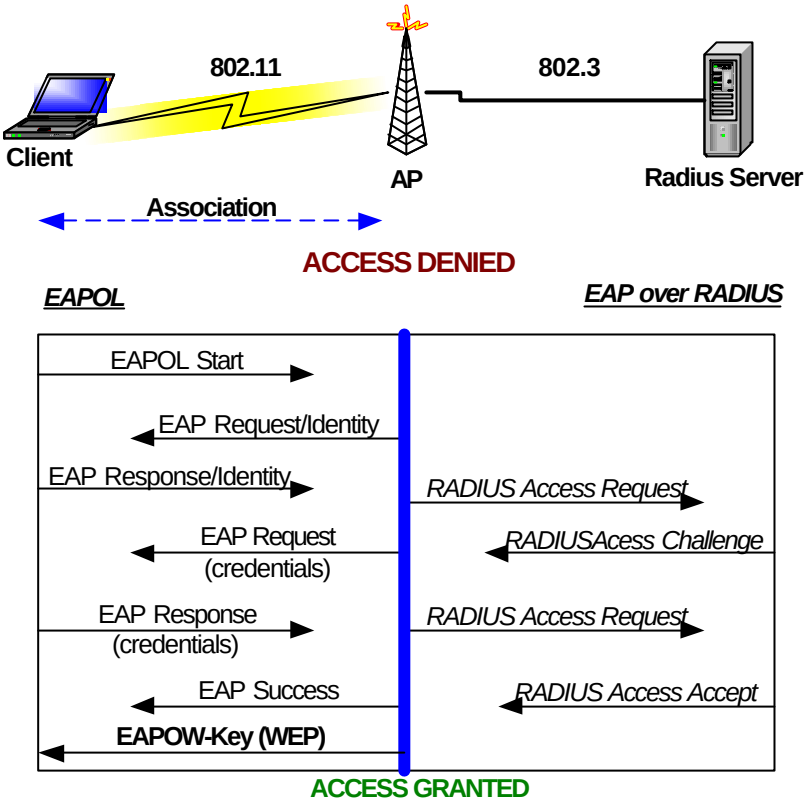

Figure 3-8 802.1X/RADIUS over an 802.11 Network

One session key can be derived for each user per session. However, if global keys (multicast/WEP keys) are used, then the session key (unicast key) sent from the AS to the AP is only used to encrypt the global key, providing per-packet authentication and integrity. An EAPOW-key packet is used for the global keys.

The 802.1X standard also supports per-station session keys, but most practical implementations only support global keys. This is because if global keys are supported, the session key is only used to encrypt the global key. The problem associated with global keys (that secrets shared among many people can lead to compromise of the secret), is solved by deploying the 802.1X per-session user keys.

Windows XP [Microsoft, 2002d] is an example of a supplicant that has integrated support for the 802.1X protocol. Its authentication types support EAP-MD5 and EAP-TLS. This platform was used in this study.

3.5.4.1 EAP-MD5

The EAP-MD5 authentication method provides one-way password-based authentication of the client performed by the AS. It is popular due to its easy deployment of passwords and usernames. However, it provides limited security, and no encryption keys are generated during the exchange. EAP-MD5 can be useful in public areas if encryption is provided at the application layer. The process is illustrated in Figure 3-9 (adapted from Orinoco [2002]).

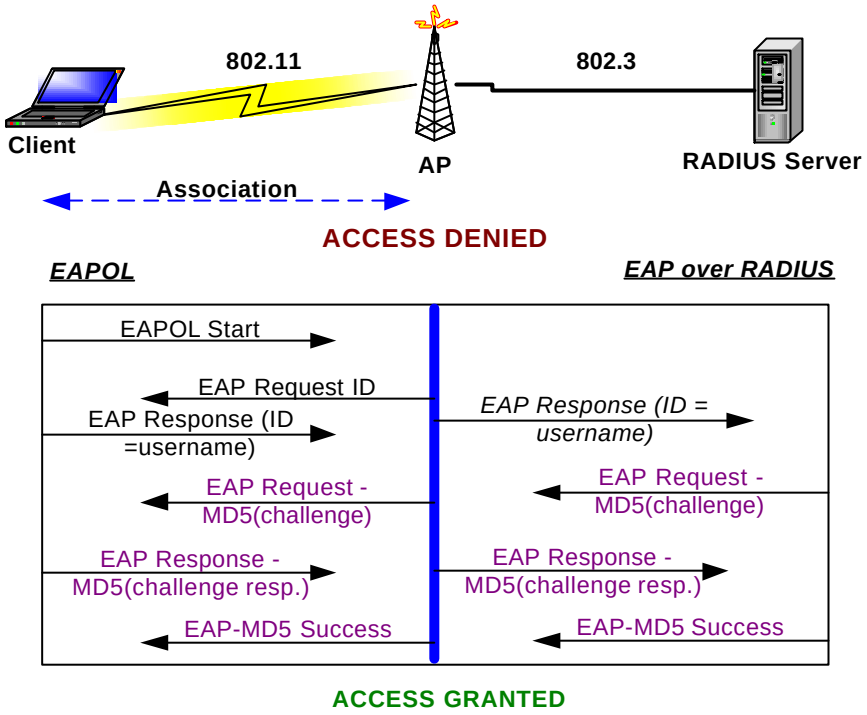

Figure 3-9 EAP-MD5 Authentication Process

3.5.4.2 EAP-TLS

EAP-TLS is the most commonly implemented EAP type for WLANs. Its authentication is based on PKI support using X.509 certificates. Both the AS and clients must possess certificates validated by a trusted authority, which ensures explicit mutual authentication. After the authentication exchange, a shared session key is generated between the AS and the client. After the AS supplies the secret key to the AP via a secured link (using EAP over RADIUS), the AS and the client can use it to bootstrap their per-packet authenticated and secured communication. Deploying EAP-TLS is complicated; thus, depending on the scale of an organisation's network, administrative burdens might outweigh the security advantages. Figure 3-10 (adapted from Orinoco [2002]) illustrates the process.

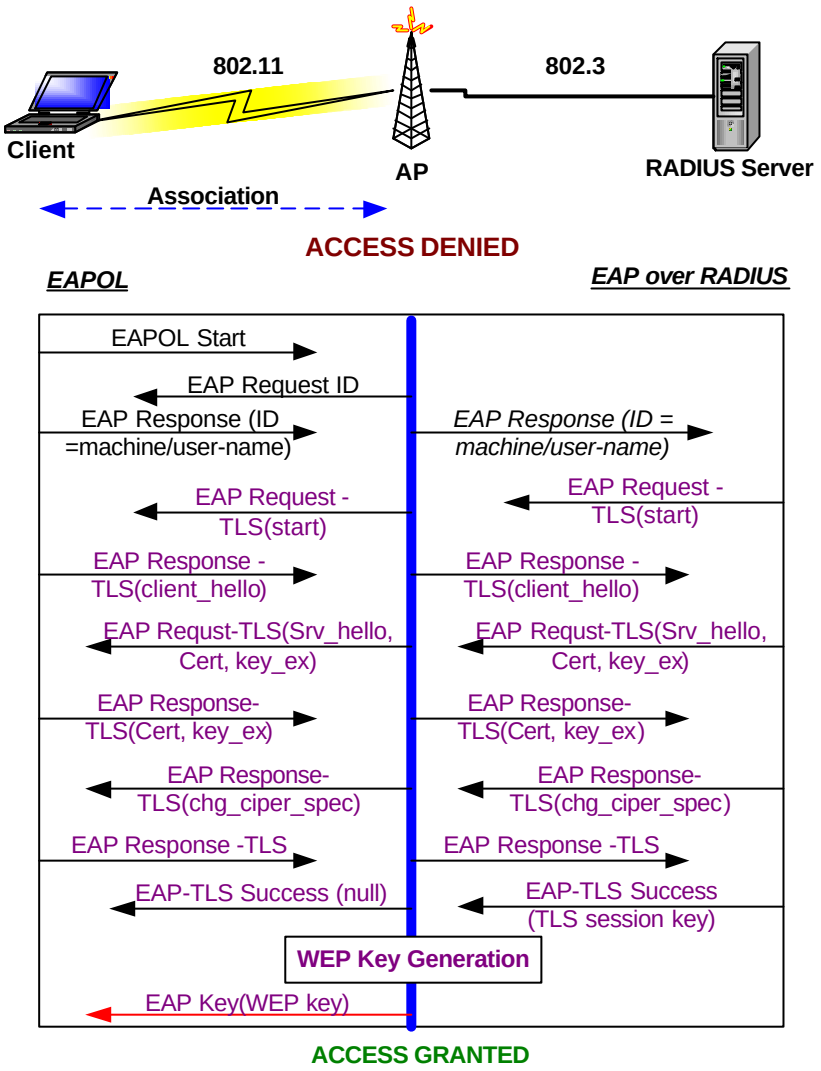

Figure 3-10 EAP-TLS Authentication Process

3.6 VPN

Virtual private network (VPN) technology is a rapidly growing security solution which provides secure data transmission over shared or public networks such as the Internet. Data is transmitted over the network by creating an encrypted, virtual, point-to-point connection between the client and a gateway VPN server that resides in a private network (Figure 3-11). VPNs provide organisations with a range of security tools to protect their internal infrastructures from external compromises [Hansen, 2001; King, 2000; Maier, 2000]. Electronic-commerce (e-commerce) deployment [Maier, 2000], for example, requires a VPN or some other extranet security protection.

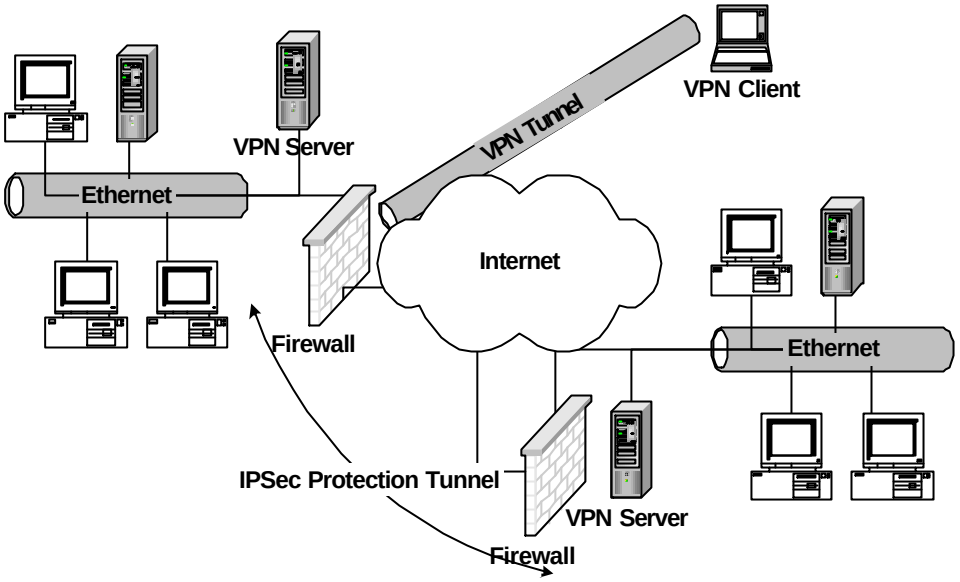

Figure 3-11 Typical VPN Implementation

VPNs can be implemented on wireless LANs in a similar manner. Several options are associated with WLAN placement:

- Placing the WLAN outside an organisation's firewall and employing a VPN to "obviate" the need for link-layer security and provide extra access control. This method might be derived from the same method used for Internet access [Maier, 2000] - treating wireless deployment as an extranet access. This approach may be expensive depending on an organisation's needs.
- Other literature [Convery & Miller, 2001; InterLink Networks, 2001; Seng, 2002] suggests enhancing the VPN with the *Internet protocol security* (IPSec) protocol by overlaying it on clear text 802.11 wireless traffic.
- Alternatively, an organisation can set up a *wireless demilitarised zone* (WDMZ) [Enterasys Network, 2002] inside the organisation's network to filter out unauthorised access. This alternative ensures end-to-end security and prevents threats such as replay and traffic analysis attacks.

Rincón [2002] provided a secured WLAN for home and *small-to-medium enterprise* (SME) users with IPSec-based VPN. As a result of this, he proposed a prototype to automate an IPSec configuration and provide nomadic mobility for users roaming

between multiple WLANs. All the WLAN clients are secured from a single workstation acting as a gateway. Caballero and Malmkvist [2002] also suggested using IPSec combined with application level access control for public WLANs.

The first two points are illustrated in the VPN structure shown in Figure 3-11 and were used in our experiment design.

3.6.1 VPN Techniques

VPNs employ a variety of security mechanisms, including cryptographic techniques and device- or user- based authentication. Tunnelling offers encapsulation (of one protocol packet inside another) for encrypted VPN traffic, so that third parties cannot view the contents of packets transported over the network.

From a technology perspective, two categories of VPN can be identified based upon whether they operate across a Layer 2 or Layer 3 network in the OSI Model. The common implementations of these two layers include the *point-to-point tunnelling protocol* (PPTP) and *layer 2 tunnelling protocol* (L2TP) at Layer 2 and the IPSec at Layer 3 [Halpern et al., 2001]. Depending on the scale of an organisation's network, and how much it values its data, both VPN security technologies can be applied. Most VPNs today make use of the IPSec protocol suite, as it ensures stronger protection against attacks. Figure 3-12 demonstrated how IPSec interacts with a WLAN.

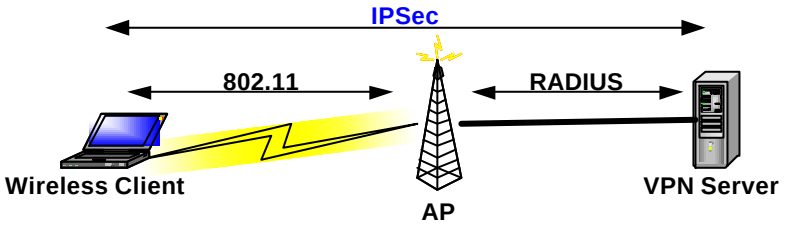

Figure 3-12 WLAN VPN Structure

3.6.2 Layer 2 VPN Technologies

As indicated above, there are two types of Layer 2 VPN technology: PPTP and L2TP.

3.6.2.1 PPTP

PPTP (RFC 2637, [Davies, 2001; Hamzeh et al., 1999]) uses a username and password to provide authenticated and encrypted communications between a client

and a gateway or between two gateways, without PKI support. The PPTP uses a TCP connection for tunnel maintenance and *generic routing encapsulation* (GRE) encapsulated PPP frames for tunnelled data. The payloads of the encapsulated PPP frames can be encrypted and/or compressed using Microsoft's proprietary encryption mechanism, MPPE based on RC4.

Authentication methods include CHAP, PAP, and MS-CHAPv2. The use of PPP provides the ability to negotiate authentication, encryption, IP address assignment, and a variety of other operational characteristics for various protocols.

3.6.2.2 L2TP

L2TP (RFC 2661, [Townsley et al., 1999]) encapsulates PPP frames to be sent over a wide range of communication types, such as IP, frame relay, or ATM networks. When configured to use IP as its transport, L2TP can be used as a VPN tunnelling protocol over the Internet. It uses UDP to send L2TP control messages for tunnel maintenance and L2TP-encapsulated PPP frames as the tunnelled data on UDP port 1701. The encapsulated PPP frames can be encrypted or compressed.

Through its use of PPP, L2TP gains multi-protocol support and provides a wide range of user authentication options, including CHAP, MS-CHAP, MS-CHAPv2 and EAP.

3.6.3 Layer 3 VPN - IPSec

IPSec, defined in RFC 2401 and 2411 [Kent & Atkinson, 1998; Rodgers, 2001; Thayer et al., 1998], provides integrity protection, authentication, and (optional) privacy and replay protection services for IP traffic. IPSec is currently the most popular protocol due to perceived security and its ability to use a single technology for both remote and Intranet/Extranet applications. IPSec sets up *security associations* (SAs), to negotiate security services between two points during the session. These SAs can be nested, allowing different IPSec relationships to be active on the same link, such as *quick mode* and *main mode*[10]. In order to establish an SA, IPSec relies on the *Internet security association and key management protocol* (ISAKMP, RFC 2408 [Maughan et al., 1998]) and *internet key exchange* (IKE, RFC 2409 [Harkins & Carrel, 1998; Maughan et al., 1998]), which defines protocol formats and procedures

[10] Microsoft Windows XP provides IPSec monitor to view these SAs.

for security negotiations, such as authentication type, encryption method, key lifetime etc.

The IPSec protocol suite specifies cryptographic support of *data encryption standard* (DES) and *triple DES* (3DES). Hashing functions can be selected from hashing functions of either HMAC-MD5 or HMAC-SHA1; HMAC-SHA1 is computationally more expensive than HMAC-MD5.

IPSec support two main architectures (and corresponding packet types):

- *Encapsulating Security Payload* (ESP) header, which provides privacy, authenticity, and integrity.
- *Authentication Header* (AH), which provides only integrity and authenticity for packets, but not privacy.

Two operational modes are provided in IPSec (see Figure 3-13):

- *Transport mode* secures an existing IP packet from source to destination. The mode allows end-to-end points to communicate over a secured tunnel, and
- *Tunnel mode* puts an existing IP packet inside a new IP packet that is sent to a tunnel end point in the IPSec format, typically between a pair of firewalls/security gateways over an untrusted network.

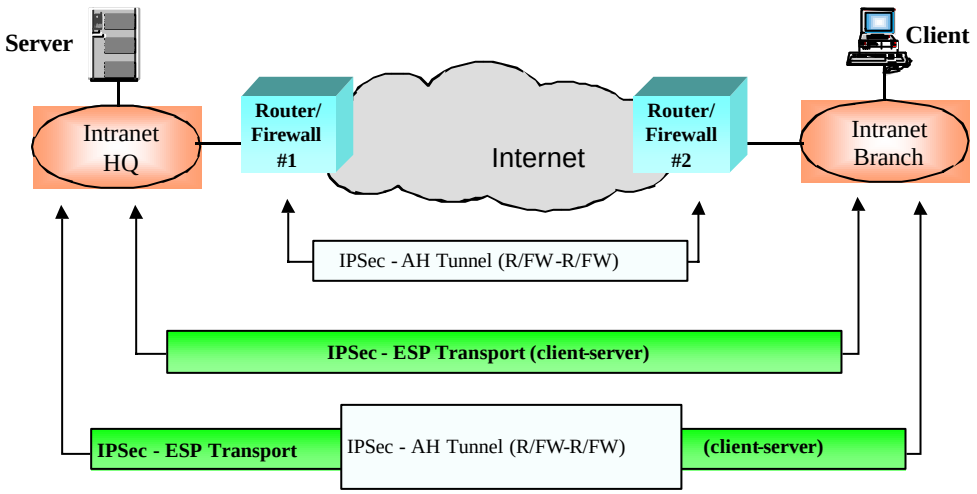

Figure 3-13 IPSec Tunnel Modes in Operation

Both transport and tunnel modes can be encapsulated in ESP or AH headers. IPSec transport mode was designed to provide end-to-end security for IP traffic between two communicating systems (for example, to secure a TCP connection or a UDP datagram). IPSec tunnel mode was designed primarily for network edge nodes, such as routers, or gateways, to secure other IP traffic inside an IPSec tunnel that connects one private IP network to another private IP network over a public or untrusted IP network. In both cases, the IKE negotiates secret keys and secured communication parameters to be used between two parties.

3.6.3.1 Device Authentications

This is also known as the machine-level authentication, which authenticates the device, not the user. The authentication methods include preshared secret key, and PKI certificates for mutual authentication. Kerberos may be used if the software provides the functionality, e.g. Microsoft Windows 2000-based networks.

The preshared secret key method does not scale well as the size of a network grows. PKI provides scalability but can be complicated to deploy. This study selected PKI as the device authentication method to carry out WLAN experiments, because PKI was also deployed for user authentication with EAP-TLS.

3.6.3.2 L2TP/IPSec provision

L2TP/IPSec provision with L2TP tunnels, RFC 3193 [Patel et al., 2001], uses the IPSec protocol suite to protect L2TP traffic over IP networks. By placing L2TP (see Section 3.6.2.2) as the payload within an IPSec packet, communications benefit from the standards-based encryption and authenticity of IPSec, as well as the interoperability to accomplish user authentication, tunnel address assignment, multi-protocol support, and multicast support using PPP. The combination, L2TP/IPSec, offers an IPSec solution to interoperable client-to-gateway VPN scenarios.

Due to incompatibilities between the IKE protocol and *network address translation* (NAT), it is currently not possible to support L2TP/IPsec or IPSec transport mode through a NAT device. Thus the deployment of IPSec transport mode should consider the requirements for NAT and scalability of access control (PKI is desirable in large scale networks).

3.6.4 Protocol Comparison

A comparison of the tunnelling technologies is presented in Table 3-2.

Feature	Description	PPTP /PPP	L2TP /PPP	L2TP / IPSec	IPSec Tunnel
User Authentication	Can authenticate the user that is initiating the communications.	Yes	Yes	Yes	Work in Progress (WIP)
Machine Authentication	Authenticates the machines involved in the communications.	Yes*	Yes	Yes	Yes
NAT Capable	Can pass through Network Address Translators to hide one or both end-points of the communications.	Yes	Yes	No	No
Multi-protocol Support	Defines a standard method for carrying IP and non-IP traffic.	Yes	Yes	Yes	WIP
Dynamic Tunnel IP Address Assignment	Defines a standard way to negotiate an IP address for the tunnelled part of the communications. Important so that returned packets are routed back through the same session rather than through a non-tunnelled and unsecured path and to eliminate static, manual end-system configuration.	Yes	Yes	Yes	WIP
Encryption	Can encrypt traffic it carries.	Yes	Yes	Yes	Yes
Uses PKI	Can use PKI to implement encryption and/or authentication.	Yes	Yes	Yes	Yes
Packet Authenticity	Provides an authenticity method to ensure packet content is not changed in transit.	No	No	Yes	Yes
Multicast support	Can carry IP multicast traffic in addition to IP unicast traffic.	Yes	Yes	Yes	Yes
* When used as a client VPN connection, machine-based authentication authenticates the user, not the computer. When used as a gateway-to-gateway connection, the computer is assigned a user ID and is authenticated.					

Table 3-2 Network Security Protocol Differences [Microsoft, 1999a]

3.7 PKI

Public key cryptography is an important technology for e-commerce, mobile-commerce (m-commerce), intranets, extranets, and web-based applications, as shown in Figure 3-14. A PKI comprises a system of certificates, certificate authorities, subjects, relying partners, registration authorities, and key repositories that provide secure and private data exchange over an unsecured network [Hunt, 2001]. The standards that define the PKI framework include X.509, *PKI for X.509* (PKIX), and the *public key cryptography standards* (PKCS). The X.509 standard defines data formats and procedures for distributing digital certificates. PKIX has been developed by IETF to support X.509-based PKI, and PKCS are a set of ongoing inter-vendor open standards produced by RSA.

Security is enforced by the use of public key cryptography, which ensures authentication, encryption, data integrity, and non-repudiation. By integrating WLANs with PKI, security is enhanced because organisations and users can be identified by digital certificates. A digital certificate acts as an electronic identification to establish the credentials of a communicating party.

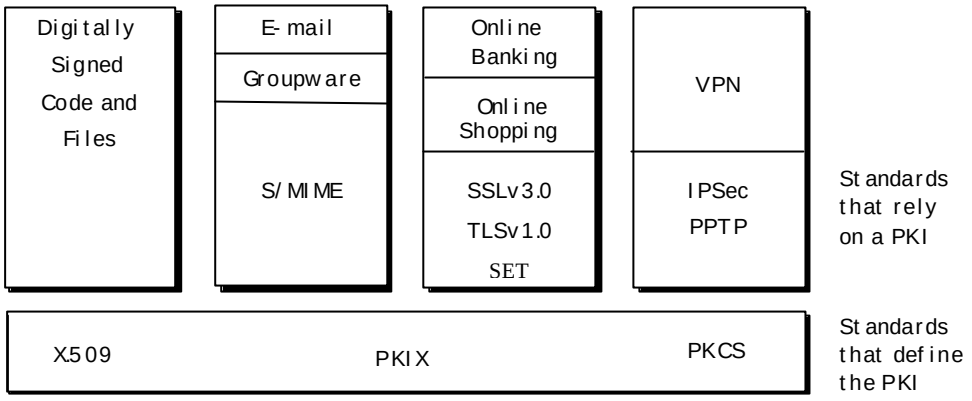

Figure 3-14 PKI Security Architecture [Hunt, 2001]

PKI provides a high level of security for users, and is the most scalable method for deploying secure shared key distribution over an untrusted network. Smartcards provide an extra level of security to PKI, as the certificates are integrated in the card to provide greater utility and portability. However, due to the complexity of its design, users need to consider the cost and administration maintenance of implementing a PKI against its benefits.

3.8 Summary

WLAN systems are beginning to incorporate a variety of new security architectures. It is important that an appropriate security mechanism is selected in order to comply with an organisation's business policy.

The security mechanisms discussed in this chapter are summarised showing their respective layers in the OSI model (Table 3-3, adapted from Caballero and Malmkvist [2002]).

OSI Layer	Name	Security Mechanism
7	Application	PKI, RADIUS, Kerberos, IPSec (IKE)
6	Presentation	
5	Session	SSL/TLS/SSH
4	Transport	
3	Network	IPSec (AH & ESP), PPTP
2	Link	802.1X, L2TP, CHAP
1	Physical	WEP

Table 3-3 OSI Model and Security Mechanisms

Polices and resources developed for remote dial-up users may be helpful because of the similarity between a wireless and a dial-up client. Both are unknown users that must be authenticated before network access is granted, and the use of an untrusted network means that strong encryption is required. The next chapter reviews network performance issues, because associating cost factors (performance) with the quality of security deployment is important and at the heart of this study.

CHAPTER 4

Network Performance

In this chapter, we discuss general performance metrics and variables, followed by an analysis of the current wireless LAN performance studies, and identify the gaps. In this chapter, we introduce the concept of treating security policies as "insurance policies", using security and performance to provide optimal solutions.

4.1 Performance Requirements

In this section, the basic concepts of network performance are defined. Many factors affect performance and some of them interact to provide overall performance results. Performance results vary depending on the choice of hardware device, software application, and network topology. Common performance measurements [Cisco, 1998; Bradner & McQuaid, 1999, Microsoft, 2000a; Yang, 2001] are as follows:

- *Response time* measures the length of time required for traffic to travel between two points. It is usually referred to as the perceived time that passes before a user receives visual affirmation [Microsoft, 2000a].
- *Throughput* is the amount of data transmitted over a network in a given time frame. It can be measured in the number of bytes per second.
- *Latency* measures the time required to send a packet that is returned to the sender (the round trip time). If the data was transmitted instantly between two points, then there is no delay at all. Latency is often used to mean any delay or waiting that increases real or perceived response time beyond the response time desired.
- *Radio signal strength* is the transmission strength of a wireless device; the higher the strength the lower the interference from items such as metal or microwaves. Distance between wireless devices also affects the radio signal strength.
- *Coverage area* considers user density in a particular area to determine the cell range of an AP. Site surveys may be required to deliver a greater throughput by overlapping coverage areas.

- *Mobility* defines how much movement between coverage areas users need.
- *User population* is the number of users in a wireless network and the quality of service expected by users. Scalability needs to be considered. For example, the number of active users per AP is critical in determining how many encrypted packets are transmitted from a user.
- *QoS* priority is given to users or data types such as voice and video.
- *Network load* is the density of a network, or how well a wireless link performs under various traffic loads. Weyuker and Avritzer [2002] studied the impact on web traffic under different loads and proposed a metric to predict network load bottlenecks under different loadings.
- *Bandwidth*, for example, the 802.11b provides the maximum capacity of 11 Mbps transmission speed.

Response time and throughput generally have an inverse relationship as network load increases [Jain et al., 1997]. RFC 1242 [Bradner, 1991] and 2544 [Bradner & McQuaid, 1999] provide a performance benchmarking methodology specifying other parameters such as packet sizes, inter-arrival packet rate, buffer control, and packet loss rate. This study conducted experiments in real-time instead of simulations; thus, only response time and throughput were used, while other variables were held constant.

4.2 Performance Evaluation

The performance of 802.11 WLANs is similar to shared Ethernets. Congestion occurs as more users are added. The theoretical throughput can be attained by using DCF (see Section 2.2.3) as 75% of the nominal bit rate [Gast, 2002], although a target of 65% is commonly observed. Applying this formula to an 11 Mbps 802.11b network, this yields a practical throughput in the range of 6 to 8 Mbps. A comparison test was carried out on the 802.11a and 802.11b throughput limits [Xiao & Rosdahl, 2002], the author observed the limit for 802.11a was 30.34 Mbps and 6.44 Mbps for 802.11b.

4.2.1 Wireless Performance

Borisov et al. [2001] stated that "Security is a property of an entire system and every decision must be examined with security in mind". Although this is certainly true, the

following studies clearly demonstrate there is a lack of attention paid to the effects of implementing security on wireless network performance.

Empirical results from Bing and Subramanian's [1998] study demonstrated that different modes of 802.11 WLAN and Ethernet frame size were crucial factors in the determination of a WLAN's transmission capabilities. The throughput of a WLAN increased as the frame length increased and as the amount of broadcast traffic decreased. Furthermore, the authors suggested that the mean response times for both wired and wireless LANs were similar, with an interframe delay of 10 ms or more. However, a broader analysis conducted in Portugal's Braganca City on its 802.11b *metropolitan area network* (MAN) found that 802.11b's effective data transmission was far from the estimated value and had a higher latency than wired Ethernet [Amaro & Lopes, 2001]. Data monitored by the *netpipe* tool showed that a 10 Mbps cross-link Ethernet peaked at 8.4 Mbps with a block size of 8195 bytes, while for wireless networks, the larger the packet size, the higher the effective rate as shown in Figure 4-1 (adapted from Amaro and Lopes [2001]). The collision avoidance mechanism of 802.11b protocol confirmed this increase, as traffic overheads introduced by the control frames *request to send/clear to send* (RTS/CTS) and the ACK frame diminished for larger packets. Their tests transferred a 1 MB file (10 times) using FTP applications with four different network paths with two cells of single or multi-hops (see Table 4-1), based on Linux operating systems. Bi-directional throughput performed 50% better than unidirectional throughput. The path with more hops reduced the throughput almost to the unidirectional level. Delay introduced by routers had more performance cost in small packet sizes than the MAC overhead. Amaro and Lopes concluded that lower throughputs produced by wireless transmission were caused by overheads introduced by physical and link layer protocols. Moreover, larger networks with more hops increased latency, but the use of overlapping channels could provide higher throughput for larger block sizes. The 802.11a shows the same characteristics of achieving higher throughput with a larger packet size, although HiperLan/2 provided a higher data rate when transmitting MPEG files [Walke, 2002].

Network Type	Network / Path	Description	Throughput (Mbps)	Block size (Kbytes)	FTP (Mbps)
Wired	Ethernet	Wired LAN	8.405061	8.002	-
Wireless	Point-to-Point (PtP)	Link between the two cells	3.694231	512	3.94
	Point-to-Multipoint (PtM)	Link inside the same cell	3.558416	383.997	3.65
	PtMtPtMtP	Link across the two cells	3.6063639	512	3.16
	PtMtP	Link inside the same cell	1.283579	48	1.34

Table 4-1 Maximum Throughputs with Different Topologies

The 802.11b product performance test conducted by Avery [2001] did not test the network performance with the security mechanism activated. Instead, he evaluated the security of each product by "looking at options available to the system manager" for securing WLANs. Thus, he did not include the operational performance effects that each product would incur. However, his test showed that the performance test should use wired 10 Mbps Ethernet network performance as a benchmark, because Ethernet and 802.11b systems have similar data transmission speeds and infrastructure.

Lezini and Mingozzi [2001] examined the performance optimisation of HiperLAN/2 by fine-tuning its capacity request and allocation mechanisms for different types of traffic. Their simulation results showed that those mechanisms had the flexibility to accommodate the QoS requirements of delay-sensitive and pulsing data traffic streams.

Chen [2001] carried out an experiment to compare the coverage area and performance between 802.11b (11 Mbps) and 802.11a (54 Mbps). He found that 802.11a provides 2-to-5-times better data-link rate and throughput performance in the same range (77 m) as 802.11b. As for co-channel interference, 802.11a produced better performance results than 802.11b. Chen also compared the trade-off between performance and costs in terms of range and total system capacity. 802.11a offered better system capacity with fewer cells (APs). With respect to security, he noted that the experiment was not subjected to "performance effects due to variability in software or higher layer protocols and applications". Thus, security issues were not investigated.

Whitmore [2001] suggested that when implementing a "secure solution", the architectural design of a network would have an effect on performance, such as a processing delay. Rodgers' study [2001] on VPNs showed that implementing security mechanisms imposed a performance cost. Significant impacts from VPN security mechanisms were incurred on routed and non-routed VPN latency measurements. By configuring security layers using a firewall, authenticated tunnels, and DES and 3DES encryption, visible effects were observed; especially there was a dramatic increase of 85% in latency for HTTP and FTP traffic in the authenticated tunnelled configuration. However, the security mechanisms of VPN had no significant impact on HTTP throughput. While very little change was experienced in FTP throughput, adding firewalls to the non-routed VPN environment caused a drop in throughput of 83.2%. Due to the nature of different network infrastructures, it was uncertain whether the security cost on performance would increase as interference increased in a wireless network environment. Our research provided an insight into wireless networks.

4.3 Size Effect

Company sizes, in terms of the number of computers, affect the way an organisation chooses to carry out its security and performance deployment. Some factors that contribute to the size effect include the vertical industry, operational models, company location, user distribution, and corporate financial health. In a survey conducted by Information Security magazine [Briney & Prince, 2002] in June 2002, the company discovered that "organisations of different sizes adhere to distinct patterns of organisational behaviour when it comes to IT security." The larger the company size, the more difficult it was to keep up with the demands of increasingly complex organisational infrastructures. Furthermore, the effectiveness of an incident recovery plan did not grow proportionally with company size. Spending money on security budgets may not reduce the level of incidents but does increase an organisation's ability to detect its loss. The survey generalised four different company sizes:

- Small (10-100 computers)

  The majority of small companies had a centralised IT organisational model with a proportional IT security budget.

- Medium (100-1,000 computers)

  These companies had proportionally poorer deployment in respect to policy, model, and budget than other groups.

- Large (1,000-10,000 computers)

  Security has become institutionalised into the corporate culture via policies. However, these companies had the most user problems regarding training and management and user-awareness.

- Very large (10,000+ computers)

  These institutions provide better policy adoption and resource allocation than large organisations, but have proportionally smaller budgets, as well as scalability issues with complex model designs, such as corporate-level and division-level policies.

The survey showed that most companies still considered malicious code and unauthorised users as the most important security problems. Organisation management remained less concerned.

4.4 Concept of Insurance Policies

Schneider [2002] addressed security through incorporating a business risk management solution. This can be achieved by enforcing liabilities and giving corporate management the means to "reduce or insure" against those liabilities. Businesses manage risks by finding adequate security at a reasonable cost, or in other words, providing a price tag to network security and allowing a company to assess its *return on investment* (ROI) in a visible format. Schneider noted that, "businesses achieve security through insurance", treating security as insurance policies bound by constraints such as standard security practices. For example, if users are concerned about denial-of-service attacks, a company can apply bandwidth interruption insurance. Premium calculation can include various factors such as money value, reputation rating, and performance costs. Security policies can be structured like fire or house insurance policies, with different customer types, classes of policies and various premium schemes. A data protection insurance policy requiring a personal software firewall, CHAP authentication, and no encryption may be offered to a small manufacturing company, costing the company a 10% performance reduction.

4.5 Summary

Various performance variables such as response time and throughput were discussed in this chapter. Prior studies showed there was a lack of performance evaluation of layered security frameworks for wireless networks. These studies concentrated on additional factors such as range or multi-hops. Other cost considerations included company size and treating security policies as insurance policies to provide incentives for better security improvement.

CHAPTER 5

Methodology

This chapter sets out the method and the environment used to conduct the experiments of this study. The aim of the experiments is to quantify the impact of security on performance of the 802.11b WLAN. The two AAA solutions for WLAN, the 802.1X and VPN, identified in Chapter 3, were selected as the two security models to assess the level of performance degradation. The 802.1X model includes the basic 802.11 standard's security using the WEP protocol and the enhanced security 802.1X standard with the EAP protocol. The VPN model includes the IPSec protocol suite for end-to-end security. A set of security layers was configured within each security model to carry out the experiment. Major differences between the two models can be identified: the VPN model requires endpoints to support the security mechanism, whereas the 802.1X model depends on the access point (acting as the authenticator) for support.

5.1 Objectives of the Research

The research goal of this study is to identify the performance and security issues of WLANs using layered security models. This goal is subdivided into three research questions:

- Is the network performance of the model at each security level the same?
- Are there any impacts on performance resulting from using the 802.1X and VPN models?
- Does security have an impact on different traffic types?

An additional outcome of the study is a proposed wireless security policy template based on the results of the experiments that provide tradeoffs between security and performance. This security policy template would become a factor in determining wireless security insurance.

5.2 Common Criteria Assessment

Common Criteria[11] is an internationally recognised method for certifying the security of IT products and systems. It defines unique security standards and establishes procedures for independently evaluating the implementation of these standards in software and other IT products. It provides a "taxonomy for evaluating security functionality" [Whitmore, 2001] through a set of functional requirements, as defined in the following eleven classes [Common Criteria 1999]:

- *Security audit:* recognises, records, stores and analyses information related to relevant security activities, e.g. remote user access information.
- *Communication:* assures the identity of parties involved in a data exchange (nonrepudiation).
- *Cryptographic support:* supports high-level security objectives and key management.
- *User data protection:* ensures user data will not be exposed to danger, via encryption and access control.
- *Identification and authentication:* establishes and verifies a claimed user identity.
- *Security management:* manages aspects of the security component such as the security component's data and attributes.
- *Privacy:* user protection against the discovery and misuse of a user's identity by other users.
- *Protection of security functions:* provides the integrity and management of the component that provides the security mechanisms.
- *Resource utilisation:* utilises the performance of the component, such as resource allocation.
- *Component access:* controls the establishment of a user session.
- *Trusted path/channel:* provides a trusted communication path between user and a security component, e.g. a secured path between a remote user and an authentication server.

[11] For more details see www.commoncriteria.org.

Common Criteria	VPN Model (IPSec)		802.1X Model (EAP)	
Security audit	√	Firewall and AS monitoring, e.g. RADIUS or Kerberos	√	AP and AS monitoring such as RADIUS
Communication	√	Digital Certificate	√	Digital Certificate (EAP-TLS)
Cryptographic support	√	IKE key management PKI DES and 3DES	√	WEP/RC4 PKI TKIP[12]
User data protection	√	DES and 3DES AS	√	WEP or AES[13] AS
Security management	√	Server	√	Server
Identification & authentication	√	AS & firewall, and user login and password; need IPSec client software	√	RADIUS server and EAP-TLS
Privacy	√	AS and VPN gateway	√	AS and AP
Protection of security functions	√	Proprietary mechanisms Firewall Physical protection	√	Proprietary mechanisms Physical protection
Resource utilisation	√	QoS Software compression	√	QoS[14]
Component access	√	IKE for session key	√	Session key moved from AS to AP over EAP-TLS
Trusted path/channel	√	Tunnelling	√	PAE control

Table 5-1 Security Architecture Evaluations by Common Criteria

The 802.1X and the VPN models have been analysed using the eleven classes of Common Criteria (Table 5-1). Both models have met all the requirements of Common Criteria, although some functions may be related to proprietary mechanisms. Furthermore, because Common Criteria enforces more stringent requirements, the five security services of the OSI model are met: namely, authentication, access control, data confidentiality, data integrity and nonrepudiation. Thus, we satisfied Whitemore's [2001] "duality of security" statement of "ensuring correct and reliable operation and protecting against error and maliciousness."

5.2.1 Product Comparison

As noted in Section 5.2, Common Criteria is a security methodology for evaluating security products and systems. An assessment of existing WLAN products is shown in Table 5-2, the three products have met Common Criteria's standards in supporting the 802.1x model The VPN model requires endpoints to support the security mechanism, whereas the 802.1x model depends on the access point (acting as the authenticator) for support.

[12] At the time of this writing, TKIP is under evaluation by the IEEE 802.11i working group.
[13] At the time of this writing, AES for 802.11 standard has been proposed but is still under development and AES-ready products are waiting for US government approval, such as a wireless manufacturer Symbol (for more details at www.symbol.com).
[14] See IEEE 802.11e workgroup on QoS deployment; currently there are several proposals for improving QoS in the MAC layer.

Common Criteria	Lucent Orinoco AP-2000	Cisco Aironet-350	3Com Access Point 8000
Product			
1. Security audit	SNMP, WEB, Telnet, Remote link test, TFTP	SNMP, WEB, Telent, TFTP	SNMP, 3Com Network Supervisor (incl.), WEB, Telnet
2. Resource utilisation	Spanning Tree Protocol (STP)	STP Cisco Discovery Protocol (CDP)	STP
3. Protection of security functions	IEEE 802.1X enabled	IEEE 802.1X enabled	IEEE 802.1X enabled
4. User data protection	40-bit or 128-bit WEP, MAC address ACL	128-bit WEP, MIC	40-bit and 128-bit WEP
5. Cryptographic support	Dynamic WEP EAP-TLS, EAP-TTLS	Dynamic WEP EAP-TLS, LEAP[15]	EAP-TLS
6. Security management	RADIUS, Certificate authentication	RADIUS, Cisco Access Control Server, Certificate authentication	3Com Network Supervisor, RADIUS, Certificate authentication
7. Identification & authentication	RADIUS, Certificate authentication	RADIUS, Cisco ACS ver.3 (not incl.)	HPOpenView, 3Com Network Supervisor, RADIUS
8. Component access	EAP-TLS, EAP-MD5, EAP-TTLS	EAP-TLS, EAP-MD5, Microsoft CHAP, LEAP	EAP-TLS, Dynamic security link with XJACK antenna on client
9. Trusted path/channel	IEEE 802.1X port	IEEE 802.1X port	IEEE 802.1X port
10.Communication	Digital Certificate	Digital Certificate	Digital Certificate
11. Privacy	128-bit RC4, RADIUS	128-bit RC4, RADIUS	128-bit RC4, RADIUS

Table 5-2 Access Point Product Comparisons

5.3 Security Configuration Levels

The experiment tested each model at different security levels. The configuration level from one (lowest level of security) to ten (highest) is shown in Table 5-3. These security levels were implemented incrementally. The security configurations include a combination of authentication, authorisation and encryption mechanisms.

5.3.1 802.1X Model

There were nine security levels selected to present a hierarchical order of the security mechanisms available from both 802.11 and 802.1X standards. Hereafter, we will refer this model as the *802.1X model*.

[15] Cisco proprietary protocol, similar to EAP

The nine security levels of this model are:

- *Level 1 No security:* this is the default security setting provided by vendors. There is no security mechanism activated with default configuration.
- *Level 2 MAC address authentication:* this level provides MAC address authentication carried out at the AP.
- *Level 3 WEP authentication:* the shared key authentication method specified in the 802.11 standard is used.
- *Level 4 WEP authentication with 40-bit WEP encryption:* this level combines the encryption algorithm to provide data privacy.
- *Level 5 WEP authentication with 128-bit WEP encryption:* the 128-bit shared key used is proprietary-based (in the case of Lucent).
- *Level 6 EAP-MD5 authentication:* this is one of the 802.1X standard's authentication methods, using password/username.
- *Level 7 EAP-TLS authentication:* this is the PKI-based authentication method supported by 802.1X.
- *Level 8 EAP-MD5 with 128-bit WEP encryption:* the combined effect of these tools provides strong data protection.
- *Level 9 EAP-TLS with 128-bit WEP encryption:* the combined effect of these tools provides the strongest level of encryption and authentication using per-session keys.

The Security Levels 2 to 5 of the 802.1X model are consistent with the 802.11 standard. Security Levels 6 to 9 are provided by the 802.1X standard.

5.3.2 VPN Model

We define the *VPN Model* based on the IPSec suite. Tunnelling is achieved by operating L2TP/IPSec (transport mode option of IPSec) and we refer to this as the IPSec tunnelling technology. This is the end-to-end IPSec solution provided by Microsoft. There are two types of authentication methods deployed in our experiments:

- Device authentication method using PKI with X.509 certificates
- User authentication methods selected based on open-standards - CHAP and EAP-TLS.

These two methods provide direct comparison with the authentication methods deployed in the 802.1X model. PPTP has been selected to provide a performance comparison with tunnelling techniques. Rincòn [2002] observed in his research that L2TP/IPSec tunnelling produced larger performance overheads than PPTP.

Ten security levels were specified:

- *Level 1 No security:* this is the default security setting. Both the 802.lX and VPN models have this in common.
- *Level 2 PPTP tunnelling with CHAP:* authenticated tunnel provided using PPTP tunnelling and CHAP authentication.
- *Level 3 IPSec tunnelling with CHAP:* authenticated tunnel using IPSec tunnel and CHAP authentication.
- *Level 4 Firewall with PPTP and CHAP:* introducing a firewall into the architecture to filter the network traffic.
- *Level 5 Firewall with IPSec and CHAP:* a firewall is introduced into an IPSec based network. From this level onward, all the security levels will be based on IPSec design.
- *Level 6 Firewall with IPSec and EAP-TLS:* applying user-based PKI with device-based certificate authentication.
- *Level 7 IPSec with CHAP and DES:* provides DES encryption to IPSec with CHAP user authentication.
- *Level 8 IPSec with EAP-TLS and DES:* applies DES encryption to EAP-TLS user authentication.
- *Level 9 IPSec with CHAP and 3DES:* provides strongest encryption (3DES) with CHAP.
- *Level 10 IPSec with EAP-TLS and 3DES:* encrypts data traffic with the strongest encryption and user authentication methods.

The VPN model can be grouped into two parts; Security Levels 2 to 4 require authentication and tunnelling using either PPTP or L2TP/IPSec before and after the firewall. Security Levels 5 to 10 requires IPSec protocol suite with a firewall to carry out authentication and encryption.

5.3.3 Security Levels of 802.1X and VPN model

Table 5-3 provides an overview of the security levels used in each model.

Level	802.1X Model	VPN Model
1	No Security (Default Installation)	
2	MAC authentication	PPTP Tunnelling & CHAP
3	WEP authentication	IPSec Tunnelling & CHAP
4	WEP (40 bit) auth. & encryption	Firewall with PPTP & CHAP
5	WEP (128 bit) auth. & encryption	Firewall with IPSec & CHAP
6	IEEE 802.1X EAP-MD5	IPSec & EAP-TLS
7	IEEE 802.1X EAP-TLS	IPSec & CHAP & DES
8	IEEE 802.1X EAP-MD5 & WEP encryption	IPSec & EAP-TLS & DES
9	IEEE 802.1X EAP-TLS & WEP encryption	IPSec & CHAP & 3DES
10	-	IPSec & EAP-TLS & 3DES

Table 5-3 Security Levels of the 802.1x Model and VPN Model

5.4 Test Environment

The testbed configuration was based upon the traditional client/server architecture but using wireless connections. The only difference was that the data transferred in the experiments were wireless. The laboratory was designed as a 'clean environment'; that is, no background noise or other interferences was present. Each model was tested separately to measure the impact on network performance.

5.5 Performance Measurements

Response time and throughput (see Section 4.1 Performance Requirements) were the parameters chosen to provide a comprehensive view of the network performance. They are defined in this research as follows:

- Response time: the total time required for traffic to travel between two points. Time is measured from the issuing of the connect command to the appearance of a disconnect message displayed by the client computer. The response time includes the time of dial-up connection establishment, security negotiation time between the client and the server and the actual transfer of the data (Figure 5-1). The time data were collected from the timestamps in the network monitoring tool.

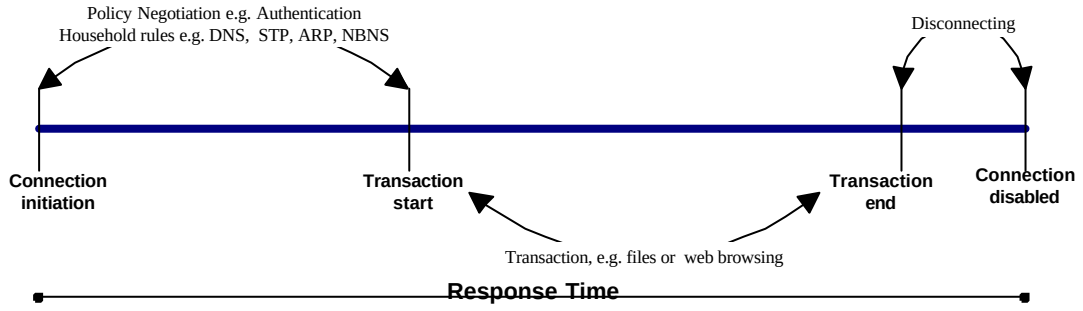

Figure 5-1 Response Time Measurement

- Throughput: the number of bytes that can be transmitted over the network in a given time period. It is the size (z) divided by the response time (t), i.e. z/t. The transmitted data sizes were collected from the network monitoring tool.

5.5.1 Application Protocol Types (FTP and HTTP)

Application protocols consist mainly of bulk data transfer (file transfer), interactive transaction (request-reply exchange) and voice data. This research was concerned with the file transfer and interactive transaction types. We were interested in the ability of a WLAN to transfer data in a predefined file size and to measure the variation in

performance when security mechanisms are implemented. FTP file transfers and HTTP transactions were selected to carry out the measurements.

The FTP file transfer utilised a single 1MB Word document from the server to the client. HTTP transactions were carried out using free software, HTTrack[16] [2002] which provides website mirroring capability. The HTTP session was defined using a mirroring link depth of four[17] on the University of Canterbury[18] website and supporting eight simultaneous user connections. The experiment would entail accessing 70 links and downloading 69 files[19] with a data size of 0.3 MB.

The FTP and HTTP transaction sizes have been chosen to represent typical and non-trivial data exchanges. The data transactions in the VPN model were not compressed in order to reflect a direct comparison against the 802.1X model.

5.5.2 Measurement Tools

Network monitoring was performed using the Ethereal [2002] application on the server. All measurements were collected from the server.

Applications used to carry out the data transaction were:

- *Microsoft FTP version 5:* a batch script to perform the transfer was written to be executed from the command line
- *HTTrack version 3.20:* this free software provided website mirroring by simulating web surfing and users downloading data.

5.6 Experiment Requirements

The general software and hardware required to carry out the experiments are described in this section. Details of system configurations for the 802.1X and VPN models are specified in Chapter 6.

---

[16] HTTrack allows user to download a web site from the Internet to a local directory, building recursively all directories, getting HTML, images, and other files from the server to a local computer. It arranges the original site's relative link-structure. Opening a page of the "mirrored" website in the user's browser, and users can browse the site from link to link, as if the user were viewing it online.
[17] Users browse websites by clicking links to go onto the related web pages.
[18] The university site was downloaded to the web server at 31 July 2002.
[19] The number of links scanned and files downloaded by HTTrack program for mirroring website link depth to four. The information was provided by the program's log at the completion of mirroring operation.

The experiment was conducted using Windows-based operating systems - Windows 2000 Advanced Server and Windows XP. Lucent Orinoco AP-2000 access point was used as the medium between the server and the client to facilitate wireless connections. The components were as follows (Appendix B describes them in more detail):

- The server used Windows 2000 Advanced Server platform to provide access controls.
- The client used the Windows XP operating system, which supported 802.1X authentications.
- The AP used the Orinoco AP-2000 product.

Transmission speeds used in the experiments:

- Between the server and the AP was a 100 Mbps Ethernet connection
- Between the AP and the client was an 11 Mbps wireless connection

5.7 Summary

In this chapter, we outlined the research objectives and the methods required to carry out our experiments. The 802.1X and VPN models were selected to measure performance degradation in the WLAN. Both models conformed to Common Criteria assessment categories, and a detailed security configuration breakdown is specified for these models. The test environment and limitations associated are discussed. Performance measurements and experiment requirements provide a general overview of the experiment structure.

CHAPTER 6

Implementation of the Security Models

In this chapter, we describe the design of the 802.1X and VPN models implemented in our experiments. These models are based on the security technology discussed in Chapter 3 and configured for our experiments as described in Chapter 5. Pilot testing was performed before the experiments to assess the usability of data collected.

6.1 System Architecture Overview

The experiment was divided into two parts, testing of the: (1) 802.1X model and (2) VPN model. On the server side, the same basic system structure was used for both models although the system architectures differed in their interaction with the RADIUS server. The NAS (Figure 6-1) took the form of a RADIUS client. In the 802.1X model, the NAS took the form of an AP, while in the VPN model it is the VPN server.

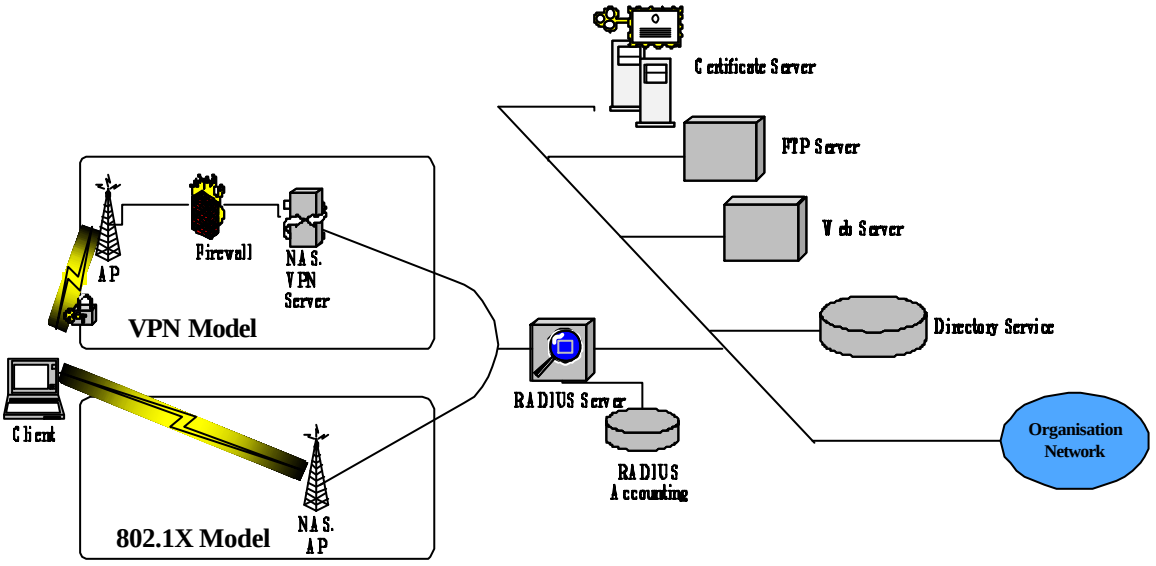

Figure 6-1 System Architecture Overview

6.1.1 Server Functionality

Using a Windows-based platform requires minimal configuration of the client machine; Windows XP has integrated the functionalities and standards of the 802.11 wireless networks. Most of our configurations were performed on the server. The server acted as

a multipurpose machine (see Figure 6-2), with the following configurations carrying out specific functions (see Appendix B for Configuration Procedures):

- *DNS server:* provides name resolution service and, in this case, functions as a domain controller.
- *Directory service:* acts as the information repository containing user, machine, group and user-specific policies based on *lightweight directory access protocol* (LDAP) technology. The application used was *active directory* (AD). AAA servers such as the RADIUS and VPN servers can be integrated with the AD to provide a single sign-on to a network.
- *Web server:* provides web monitoring and control using Microsoft *internet information service* (IIS).
- *FTP server:* provides file access and transfer control using Microsoft FTP server.
- *Network monitor:* monitors the network traffic using Ethereal.

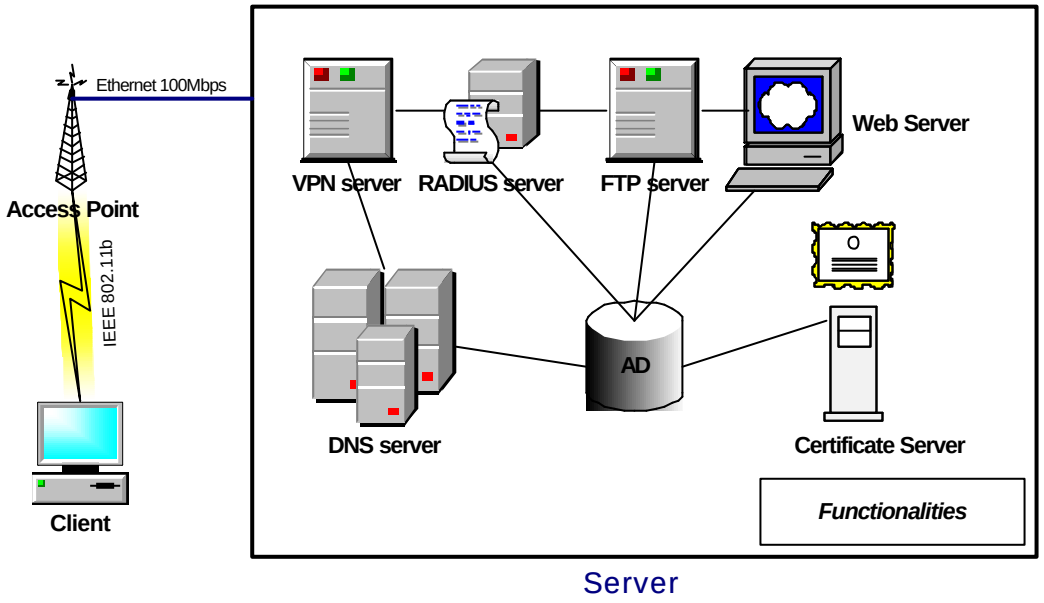

Figure 6-2 Logical Functionalities of the Server

Three additional installations were required for both models:

- *RADIUS server:* provides authentication and accounting remote users based on their credentials.
- *Certificate authority (CA,* also known as certificate server*):* issues and maintains user and computer certificates.

- *VPN server:* provides remote access control and monitoring of VPN users using Microsoft *remote access server* (RAS).

An organisation may wish to deploy a DHCP server to perform automatic IP address issuing to wireless users. However, in Chapter 3, we discussed the vulnerabilities of using a DHCP server for wireless networks; thus, a DHCP server was not included in our design.

6.1.2 Remote Access Policy Structure

A directory-enabled network allows a network to be managed and controlled centrally; thus, policy deployment is carried out from the domain controller to the overall network. The network administrator can define and create remote access policies to control the level of remote access that a user or group of users has in Windows 2000 Advanced Server. Users can be controlled and managed based on their roles and group association; for example, a user Ada Cornwell can have multiple roles and privileges (Figure 6-3). Remote access policies are a set of conditions and connection settings that must be met by users in order to gain network access. Using Group Policy (see Appendix B) in the AD centralises remote access policies in a network.

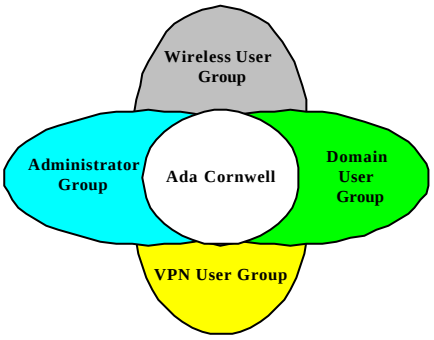

Figure 6-3 User and Groups

The RADIUS server or the VPN server can perform remote access control monitoring. Access control is enforced based on policies, either group- or user-specific. Integrating with the directory allows both servers to verify user identities and access authority. In Windows design, the user-specific policies in the directory override the policies defined in both servers (Figure 6-4). In the 802.1X model in our experiment, the RADIUS server and the AP formed the access control management. In the VPN model, the integration of the RADIUS server and the VPN server formed the network management team.

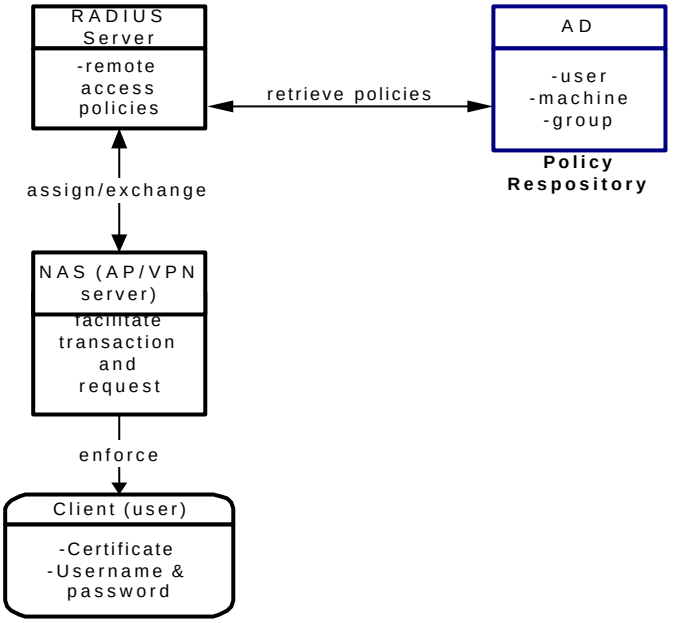

Figure 6-4 Policy Structure

The policy evaluation logic is illustrated in Figure 6-5 (adapted from Microsoft [1999b]). A wireless user is authenticated and connected to a network if a user has the permission and the right credential to access the network. The security communication mechanism used can be either the port-based 802.1X authentication or the tunnelled IPSec access.

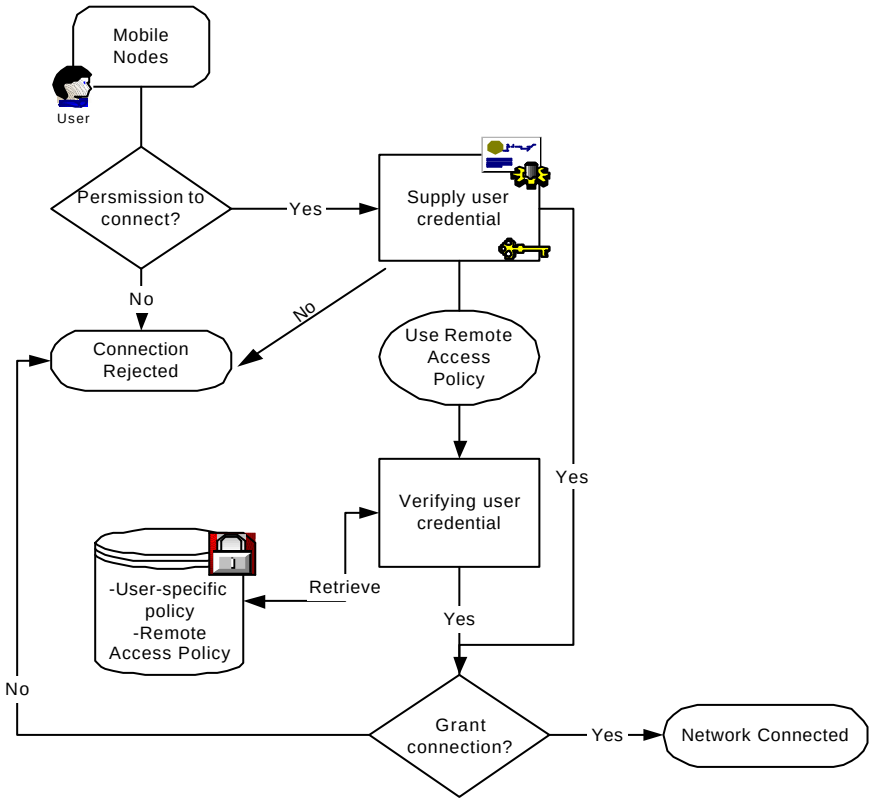

Figure 6-5 Policy Evaluation Logic Flow

6.2 802.1X Model Implementation

The 802.1X model consisted of the 802.11 access mechanism using open and shared key authentication, WEP encryption, and the 802.1X port-based authentication. By combining 802.1X with 802.11 protocols (as security levels 6 to 9, see Table 5-3), the model provided a controlled wireless network with user identification, centralised authentication, and dynamic key management.

The 802.11 access mechanism was tested for security levels 2 to 5. Static key management and basic network access was facilitated by the access point. For security levels 6 to 9, the integration of 802.1X and 802.11 provided a dynamic key management and centralised authentication by the RADIUS server (Figure 6-6). Authentication methods chosen for the experiment were the EAP-MD5 and EAP-TLS; other proprietary authentication methods such as EAP-TTLS were not considered. This model did not support end-to-end security, because privacy and confidentiality were only ensured on the wireless link by the WEP, but not enforced on the wired counterparts.

Wireless users were treated as if they existed in one subnetwork in an organisation's intranet. A specific IP address was assigned to the wireless user, AP, and different components of the server.

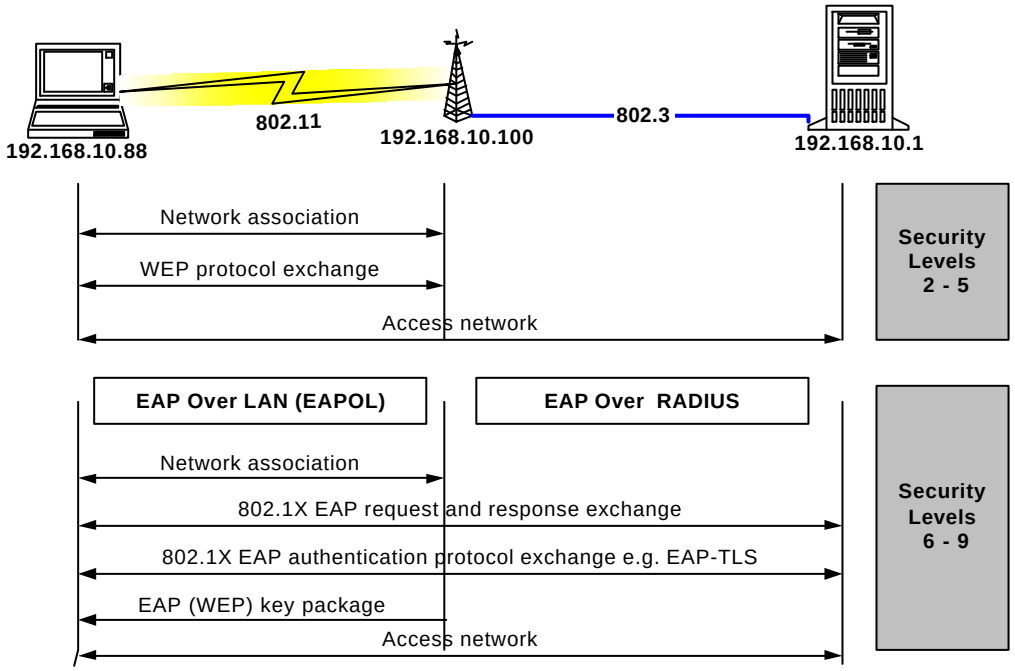

Figure 6-6 802.1X Model Logical Flow

RADIUS server and certificate authorities were added to the basic network structure to provide the 802.1X authentication support (Figure 6-7). The RADIUS server supported wireless user sign-on, and a certificate authority was used to issue certificates to users for EAP-TLS authentication.

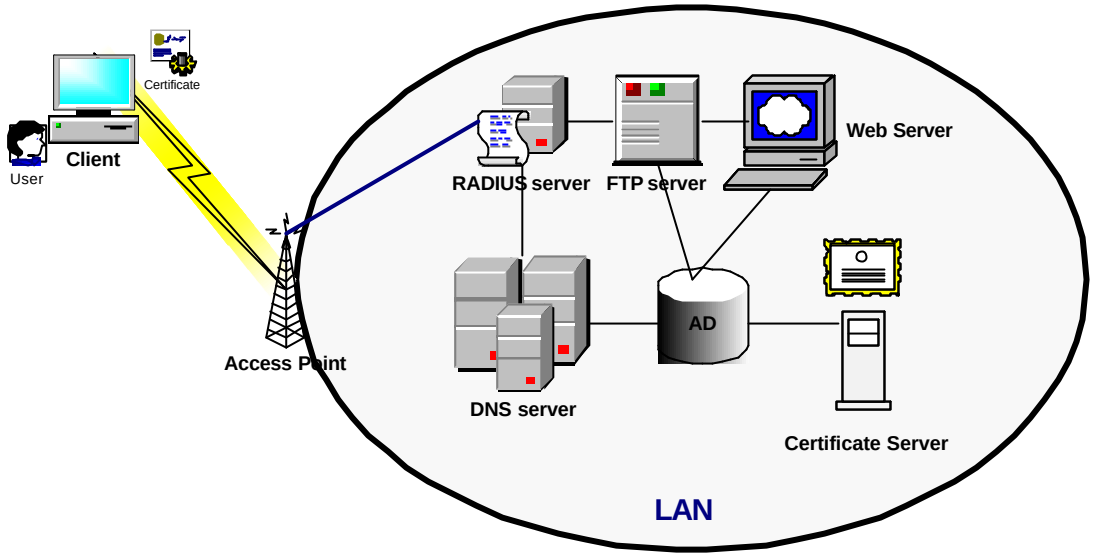

Figure 6-7 802.1X Model Implementation

6.2.1 Remote Access Policies

In the 802.1X model, the RADIUS server and its client, AP-2000, performed the policy check and authentication. Policies are effective after the activation of the RADIUS server. The 802.1X standard specifies the use of RADIUS server for enhanced user authentication. In the 802.1X model, RADIUS server was activated after security level 5 (see Section 5.3). The following remote access policies are based on this point.

- General wireless access to the Intranet (see Appendix C)
- Wireless user groups can access the organisation's intranet via IEEE 802.11 wireless transmission. Access can be further split into two policies for stricter control:
    - Wireless access control using EAP-MD5
        - ✓ Access is granted to an organisation's intranet if the wireless user possesses the right username and password, e.g. User Ada has been authenticated with login name ada@canterbury.ac.nz and password[20].

[20]EAP-MD5 (equivalent to CHAP) requires the user password to be stored in reversible encrypted order; see Appendix B.

- Wireless access control using EAP-TLS
    - ✓ Access is granted to an organisation's intranet if the wireless user possesses the correct X.509 digital certificate, e.g. User Ada has been authenticated with her digital certificate "Ada Cornwell"

6.3 VPN Model Implementation

The VPN model deployed the IPSec mechanism to support an end-to-end secured communication from wireless to wired links. Tunnelling protocols used were IPSec and PPTP. Most of the testing was based on the IPSec mechanism. However, as PPTP is a popular VPN tunnelling choice used by organisations, we tested the effect of using PPTP tunnelling against IPSec at the early stage of the model. PKI was selected over preshared keys to identify a user, and X.509 certificates were used for distributing and authenticating the keys. User authentication alternatives elected were CHAP and EAP-TLS. Chapter 3 explained that CHAP authentication is equivalent to EAP-MD5 authentication.

User authentication and tunnelling options were tested before and after the firewall installation in security levels 2 to 5. From there onwards, IPSec was the sole security protocol used with different user authentication alternatives. Security level 3 and levels 5 to 10 provided both user and device authentications. Encryption mechanisms such as DES and 3DES were used to ensure end-to-end data protection. The network was divided into subnetworks and treated the wireless subnetwork as an extranet (Figure 6-8).

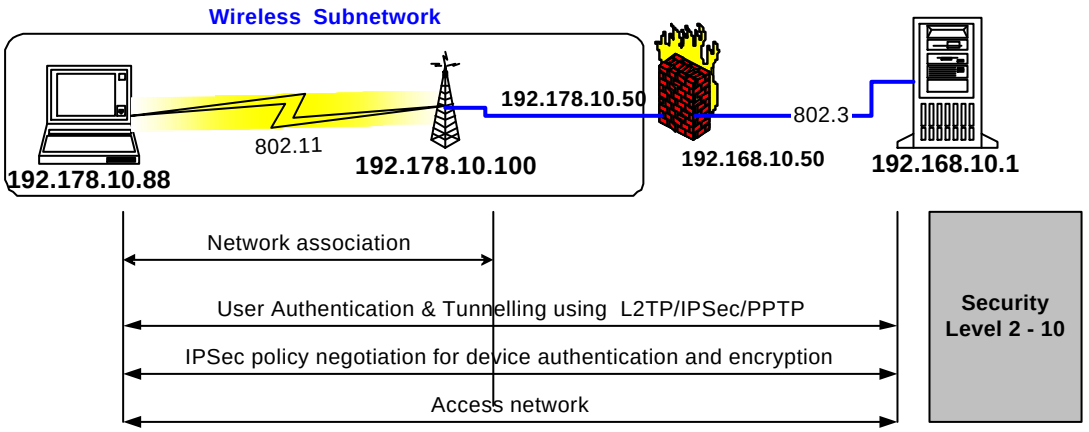

Figure 6-8 VPN Model Logical Structure

6.3.1 Additional Components

In the VPN model, additional components were introduced into the network: RADIUS server, VPN server, certificate authority, and a firewall (Figure 6-9). The RADIUS server and certificate authority were installed during the 802.1X model experiment; thus, only a VPN server and a firewall were newly implemented (See Appendix B).

We configured the VPN server to be the RADIUS client and a software firewall was set up between the access point and the VPN server. A hardware firewall was originally our first choice; however, vendor product interoperability issues occurred. Thus, a software firewall was implemented.

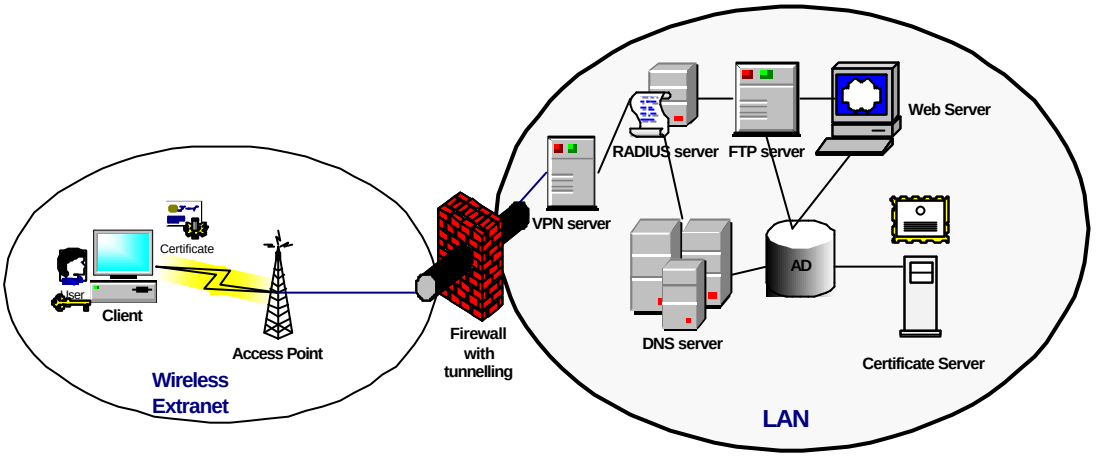

Figure 6-9 VPN Model Implementation

6.3.2 Remote Access Policies

In this model, the two types of access polices, device and user authentication, are defined. Device authentication is performed by the IPSec functions inside the VPN server using customised IPSec policies (see Section 3.6.3 IPSec). The automatic IPSec policy *L2TP Rule*[21] provided by Microsoft was disabled because it provides HMAC-MD5 as the hashing algorithm. Our customised IPSec policy allowed us to specify the use of a more secure hashing algorithm, HMAC-SHA1. The RADIUS server and the VPN server (RADIUS client) use policies similar to those specified in the 802.1X model in order to carry out user authentication. Furthermore, software compression was not used in the VPN model thus a direct comparison of transferred data size between the two models could be made.

[21] For more information about how to use or disable this automatic rule, see Microsoft Knowledge Base Q248750 and Q310109.

6.3.2.1 IPSec Policy

Our customised IPSec policy (see Appendix C) was assigned on both the server and the client machines.

- Secure Remote Access
- Policy negotiation requires a certificate authentication and HMAC-SHA1 hashing algorithm.
    - We used the customised filter with policy priorities of:
        - ✓ ESP [3DES, HMAC-SHA1]
        - ✓ ESP [DES, HMAC-SHA1]
        - ✓ ESP [No encryption, HMAC-SHA1]

6.3.2.2 User Access Policy

User access policies were specified according to our experiment requirements.

- General VPN access to the Intranet (see Appendix C)
- The VPN user group (including the Wireless user group) can access the organisation's intranet via a VPN connection. Access can be further split into two policies for stricter control:
    - VPN access control using CHAP authentication
        - ✓ Access is granted to an organisation's intranet if the VPN user possesses the right username, password and encryption type, e.g. User Ada has been authenticated with login name ada@canterbury.ac.nz, and a password, and 3DES encryption is used to protect the data transmission.
    - VPN access control using EAP-TLS authentication
        - ✓ Access is granted to an organisation's intranet if the VPN user possesses the right digital certificate and encryption type, e.g. User Ada has been authenticated with her digital certificate "Ada Cornwell", and 3DES encryption is used to protect the data transmission.

6.3.2.3 Firewall Rules

A firewall was introduced in the VPN model; thus, associated rules need to be defined. Data transmissions are encapsulated; therefore, we only need to specify ports to enable the tunnelling and encapsulated data.

- VPN Transactions [Microsoft, 1999a]
    - UDP port 500 on both the inbound and outbound interfaces.
    - TCP port 1723 on both inbound and outbound interfaces.
    - Trust the IP address of the server and the client (or the IP port ID of 40, 50, and 51).

6.4 Pilot Testing

During our implementation of the 802.1X model, we conducted a pilot test to assess the feasibility of our measurement point and test run numbers. The security levels tested were levels 1 to 5. Three tests were run for both FTP and HTTP traffic. The FTP transaction used five different file types to test the response time and throughput: text (50Kb) and Word document (1MB), and three multimedia files were used: PDF (5.95MB), MP3 (3.81MB) and MPEG (40MB). The HTTP transaction was tested with a single session surfing 70 links and downloading 69 files with total size of 333Kb. This HTTP transaction size was decided to present adequate user web surfing usage after a few adjustments to define the transaction size.

Results from the FTP testing showed that throughput decreased when WEP authentication and encryption (40-bit and 128-bit) were implemented at levels 3 to 5. Multimedia file types provided a more visible degradation, with decreased throughput and increased response time. This could be due to the large file size and data type. The HTTP results showed that WEP authentication (level 3) and 128-bit WEP authentication and encryption (level 5) have impacts on performance. In addition, MAC address authentication (level 2) had a slight impact on performance.

Overall, the results from the pilot test showed that performance degradation was experienced with WEP authentication and encryption for both the FTP and HTTP application protocols. However, at certain security levels, the impacts were insignificant and some security levels did not fulfil our security assumptions that the higher the security is, the higher the performance overheads. Analysis and reporting on the full experiments and their outcomes is covered in Chapter 7.

Our investigation found that system factors, such as disk paging and memory caching, played a role during our testing period, because outlier data were collected. Research

carried out by Amaro and Lopes [2001] addressed similar issues by discarding the first file transfer, and allowing the file to be placed on the sender's file system cache. We decided that three test runs for each file were not enough to accurately assess the models, due to the system factor influences. Thus, the experiment would be conducted using fifteen test runs, and the first five would be discarded to exclude system factors. The FTP file type was limited to a single Word document file to provide a more manageable data size.

6.5 Summary

In this chapter, we describe the separate implementation of two types of WLAN security models. Specific remote access policies were defined for each model to carry out the authentication, authorisation, and encryption mechanisms. Initial results from the pilot test showed that test runs needed to be carried out to remove system factors from the test environment. A secured WLAN must be balanced with performance to achieve an optimised solution.

CHAPTER 7

Experimental Evaluation and Analysis

In this chapter, we quantify the level of performance overhead incurred when implementing the different security mechanisms specified in Chapter 5. More specifically, we try to address the effect of security levels, models, and traffic types on performance. Data analysis was carried out by experimenting with different security mechanism deployment, and various combinations of these mechanisms. The statistical tools, *analysis of variance* (ANOVA) and t-tests (see Cooper and Schindler [2001] for analysis instruments), were used to analyse the data collected from the experiment. The analysed results will be combined with the security recommendations discussed in Chapter 3, as well as other performance parameters in Chapter 4, in order to build wireless security strategies.

7.1 Experimental Result Overview

The experiments followed the two models described in Chapter 5 - the 802.1X model and VPN model. An infrastructure mode of operation and a single cell were used with a single client. Performance measures were gathered by running ten repetitive tests with different security configurations for each model (see Appendix A Captured Data). FTP and HTTP traffic were captured by the Ethereal monitoring tool. Data were analysed, at the corresponding 95% confidence interval.

Our research questions were constructed into the following null and alternative hypotheses:

- There is no difference between the models implemented to secure WLAN transmission. The alternative hypothesis is that the VPN model presents more performance degradation than the 802.1X model. Statistical tests were performed using the *t*-test.
- There is no difference between traffic types, while the alternative hypothesis assumes there is a difference. Statistical tests were performed using the *t*-test.

- There is no difference between security mechanisms applied in each model; while the alternative hypothesis assumes there is a difference. Statistical tests were performed using ANOVA and were followed by various *t*-tests.

7.1.1 Retesting

The data collected from the VPN model experiments showed surprising results. The results observed from security levels 4, 5, and 7 to 10 did not follow our assumptions that stronger security mechanisms have a greater performance impact. In particular we found that:

- Implementing a firewall *improved* network performance.
- CHAP user authentication *increased* response time more than EAP-TLS authentications.
- 3DES encryption *improved* the HTTP throughput compared to DES encryption.

A retesting was carried out on these security levels to investigate the causes. We decided to reboot the machines each time an IPSec policy was changed, thus avoiding previous IPSec policy presence. Comparison made on the data collected before and after retesting found that only the firewall security levels produced approximately the same results as before; other security levels followed our assumptions. Thus, we concluded that when implementing different IPSec policies/filters, for example if a user changed from DES to 3DES then the device should be restarted to avoid residual effects from previous policy implementation.

7.2 Impact of Model Choice

The results collected from the experiment rejected the null hypothesis and indicated that the VPN model produced higher performance overheads (see Table 7-1). Figures 7-1 and 7-2 illustrate that the VPN model, on average, had longer response times and lower throughputs for FTP and HTTP traffic.

Model	**802.1X Model**		**VPN Model**	
(Mean)	Response Time	Throughput	Response Time	Throughput
FTP	19.092	84454.360	45.632	39336.222
HTTP	25.571	19723.388	50.951	12054.027

Table 7-1 Mean Response Time and Throughput of the Two Models

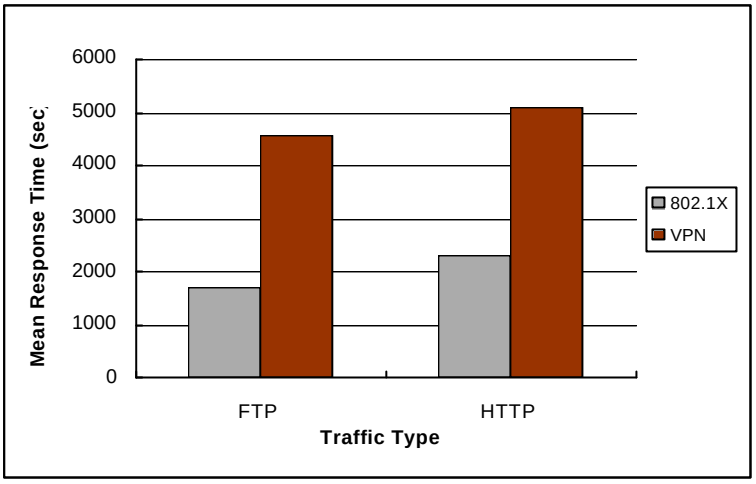

Figure 7-1 Mean Response Times in the Two Models

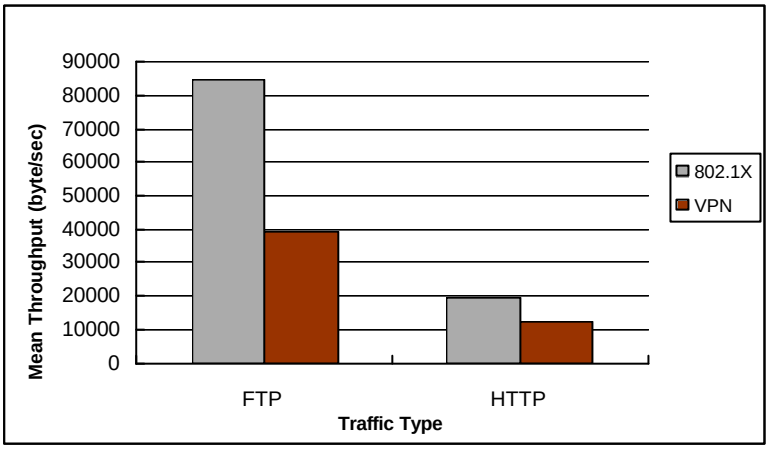

Figure 7-2 Mean Throughputs in the Two Models

The *t*-tests carried in Table 7-2 indicated that deploying different models to secure wireless transmission significantly affected the performance at $p < 0.0000$, regardless of which application protocol was used. The VPN model had more than doubled the response time for both FTP and HTTP traffic. The 802.1X model provided a much better throughput for FTP traffic. Implementing the security technologies of tunnelling, firewalls, device-based certificate authentication, sophisticated key exchange, and encryption algorithms contributed to these performance degradations.

Model	**FTP**		**HTTP**	
	Res. Time	*Throughput*	*Res. Time*	*Throughput*
***t*-statistics**	-9.1813	8.6089	-9.1132	8.4091
p*-value	*0.0000*	*0.0000*	*0.0000*	*0.0000*

*Two-tailed at a = 0.05

Table 7-2 Model Comparison of 802.1X and VPN in FTP and HTTP Traffic

7.3 Impact of Traffic Type on Performance

Each model used two types of application protocols to transfer data: FTP and HTTP. FTP is used to transfer bulk file data, while HTTP exchanges a series of request-reply messages during the transmission period. In each model, the FTP response time and throughput were compared against HTTP. Table 7-3 illustrates the impact on performance using different traffic types within each model, the *p*-values were smaller than the alpha value of 0.05, and this indicated that type of traffic used significantly affected overall network performance. FTP performed better than HTTP, with faster response time and greater throughput, as shown in Table 7-1. The table also proved the point made in Section 7.2, that the 802.1X model performed better than the VPN model. Due to the nature of these transmission techniques and the different sizes of file used, this table provides only a limited view. For more detailed analyses of traffic type impacts, see Section 7.4.

Traffic	**802.1X Model**		**VPN Model**	
	Response Time	Throughput	Response Time	Throughput
t-statistics	-28.0239	17.4831	-9.7957	11.5024
p-value*	*0.0000*	*0.0000*	*0.0000*	*0.0000*

*Two-tailed at a = 0.05

Table 7-3 FTP vs. HTTP Performance in the Two Models

7.4 Impact of Security Levels

The data collected from experiments were evaluated by ANOVA, testing the overall impact of the various variables (security levels with regards to traffic types) on performance in the two models. However, ANOVA does not provide explanations for the differences or a detailed understanding of the interactions. Deploying paired t-tests provides a more detailed analysis of the impact on performance from different security levels.

7.4.1 Overall Differences Among Security Levels

There were four two-way ANOVA tests conducted to determine the overall security levels and traffic type impact within each model. The ANOVA tested two factors – security levels (in each model) and traffic type, and considered the effects of these two factors jointly to see if there was an interaction effect. Significant interaction effects between these two factors were found at the 0.05 level for each model, as shown in Table 7-4. Therefore security levels and traffic type jointly impact network performance

(response times and throughputs). Thus, the individual main effects (from each factor) on performance could not be considered separately. In other words, when testing impact on performance, security level and traffic types need to be considered jointly.

ANOVA	802.1X Model				
		Response Time		Throughput	
	df	*F ratio*	*p-value**	*F ratio*	*p-value**
Security Levels (e)	8	2737.25	*0.0000*	692.14	*0.0000*
Traffic Types (f)	1	1542.53	*0.0000*	14662.81	*0.0000*
Interaction (e*f)	8	12.91	*0.0000*	451.67	*0.0000*
	VPN Model				
		Response Time		Throughput	
	df	*F ratio*	*p-value**	*F ratio*	*p-value**
Security Levels (e)	9	1600.16	*0.0000*	997.31	*0.0000*
Traffic Types (f)	1	164.80	*0.0000*	5647.17	*0.0000*
Interaction (e*f)	9	10.31	*0.0000*	458.92	*0.0000*

*Two-tailed at a = 0.05

Table 7-4 ANOVA Analysis of Overall Security Levels

The results of ANOVA provide sufficient empirical evidence that there were performance differences among security levels used in each model (see descriptive statistics in Table 7-5 for 802.1X model and Table 7-8 for VPN model). The response times and throughputs of traffic types (FTP and HTTP) showed that security levels significantly differ from each other in their effect on performance (*p*-value <0.0000); see Table 7-4 for details. The data used for ANOVA analysis were based on Appendix A Captured Data.

7.4.2 Security Mechanisms of the 802.1X Model

Following the rejection of our null hypothesis that there are no differences in performance among security levels, we further investigate the impacts and interaction of each security level in the 802.1X model. The mean level and standard deviation of response time and throughput observed on each of the security level are given in Table 7-5, while Table 7-6 presents the overview of different paired t-tests. Table 7-5 provides abbreviated information on each security level; for more details refer to Table 5-3 in Chapter 5.

802.1X Model	Response Time(sec)				Throughput(bytes/sec)			
Security Level	FTP		HTTP		FTP		HTTP	
	Mean	*Std. Dev.*	*Mean*	*Std. Dev.*	*Mean*	*Std. Dev.*	*Mean*	*Std. Dev.*
1. No Security	9.618	0.686	16.721	1.136	117890.65	8348.549	25487.72	1730.131
2. MAC A.	9.174	0.430	16.407	0.996	122969.98	5566.224	25824.15	1539.270
3. WEP A.	8.911	0.393	17.768	0.687	126664.58	5767.990	23887.46	924.744
4.WEP A+E(40)	9.002	0.611	17.001	0.893	126001.48	8757.337	25143.60	1279.126
5. WEPA+E(128)	10.783	0.785	17.078	1.565	105059.29	7386.367	25094.41	2189.589
6. MD5 A.	20.544	1.450	24.665	1.570	55153.62	4090.844	17201.31	1155.156
7. TLS A.	22.909	2.409	26.176	1.130	49899.18	5168.803	16272.91	675.036
8. MD5 A+E(128)	39.751	0.398	46.889	0.817	28707.79	271.962	9438.67	194.491
9. TLS A+E(128)	41.135	0.719	47.434	1.120	27742.67	471.077	9160.26	238.217

Table 7-5 Descriptive Statistics of 802.1X Model

The paired ttests carried out in Table 7-6 used *Pair* numbers to identify the tests evaluating two specific groups. We selected these ten pairs instead of carrying out all the t-tests for every security level because some security levels are mutually exclusive, and the hierarchical nature of the model can provide related results on the higher security levels. The reasons for choosing each pair are as follows:

- Pair 1 – compares the MAC address authentication against the default setting (no security protection at all). The default security setting requires comparison with only one security level, as previous results in ANOVA have identified that there are differences among security levels already. Results from Pair 1 will help us make some hierarchical assumptions about default security against the remaining eight security levels.
- Pair 2 – compares the differences between MAC and WEP authentication impact.
- Pair 3 – compares the impact of deploying 40-bit WEP encryption with simple WEP authentication.
- Pair 4 – compares the authentication methods from the 802.11 and 802.1X standard, more specifically EAP-MD5 against WEP.
- Pair 5 - compares the differences between different key lengths of 40- and 128-bits used by the WEP protocol.
- Pair 6 – compares the difference between two authentication methods when both used 128-bit WEP encryption.
- Pair 7 – compares the password based authentication, MD5, and the certificate based authentication, TLS.
- Pair 8 – evaluates the impact of adding WEP encryption onto the EAP-MD5 authentication method.
- Pair 9 – compares the differences between EAP-MD5 and EAP-TLS authentication when combined with WEP 128-bit encryption.

802.1X Model		Response Time				Throughput			
	Security	FTP		HTTP		FTP		HTTP	
Pair	Levels	*t-stats*	*p-value**	*t-stats*	*p-value**	*t-stats*	*p-value**	*t-stats*	*p-value**
1. No Sec vs MAC	1 vs 2	1.5682	0.0756	0.8194	0.2168	-1.4510	0.0904	-0.6218	0.2748
2. MAC vs WEP A.	2 vs 3	1.6628	0.0654	-3.0733	*0.0066*	-1.6615	0.0655	3.0013	*0.0075*
3. WEP for E.	3 vs 4	-0.3913	0.3523	2.0521	*0.0352*	0.1962	0.4244	-2.3932	*0.0202*
4. WEP vs MD5 A.	3 vs 6	-22.9647	*0.0000*	-12.8921	*0.0000*	28.6970	*0.0000*	15.0648	*0.0000*
5. WEP E.40 vs E.128	4 vs 5	-6.8860	*0.0000*	-0.1280	0.4505	7.0540	*0.0000*	0.0591	0.4771
6. WEPvs MD5 A.&E.	5 vs 8	-110.9027	*0.0000*	-55.0430	*0.0000*	32.8324	*0.0000*	22.4167	*0.0000*
7. MD5 vs TLS A.	6 vs 7	-2.9566	*0.0080*	-3.0331	*0.0071*	2.7835	*0.0106*	2.4978	*0.0170*
8. MD5 for E.	6 vs 8	-37.9875	*0.0000*	-40.9776	*0.0000*	20.2079	*0.0000*	22.2382	*0.0000*
9. TLS for E.	7 vs 9	-2.2191	*0.0127*	-39.1071	*0.0000*	13.1118	*0.0000*	29.6240	*0.0000*
10. MD5 vs TLS A&E.	8 vs 9	-5.7881	*0.0001*	-1.1870	0.1328	6.0931	*0.0001*	2.7806	*0.0107*

*One-tailed at a = 0.05

Table 7-6 802.1X Security Performance Comparison

The *Pair* ordering for the t-test comparisons in Table 7-6 were based on the level of security protection from the lowest protection level (1) to the highest (10). The following analysis were also organised on the level of security quality, thus some of the *Pair* numbers would not be in order in certain sections. The percentage change calculated for each *Pair* comparison was based on Table 7-5's mean values.

7.4.2.1 Impact of MAC Authentication

When the AP was configured to provide MAC address authentication to wireless clients, there was no significant change in the response time and throughput of FTP and HTTP. In Table 7-6, *Pair 1* shows that p-values for response time of FTP (p = 0.0756) and HTTP (p = 0.2168) are greater than 0.05. Similar results occurred for the throughput of FTP (p = 0.0904) and HTTP (p = 0.2748). The data used for comparison is shown in Table 7-7 (extracted from Table 7-5).

802.1X Model	Response Time(sec)				Throughput(bytes/sec)			
Security Level	FTP		HTTP		FTP		HTTP	
	Mean	*Std. Dev.*	*Mean*	*Std. Dev.*	*Mean*	*Std. Dev.*	*Mean*	*Std. Dev.*
1. No Security	9.618	0.686	16.721	1.136	117890.65	8348.549	25487.72	1730.131
2. MAC A.	9.174	0.430	16.407	0.996	122969.98	5566.224	25824.15	1539.270

Table 7-7 No Security and MAC Address Authentication Comparison

Because the t-tests results indicate that no significant performance degradation when the MAC address authentication is deployed, the MAC address authentication should be used whenever possible to provide an extra measure of protection.

7.4.2.2 Impact of WEP Authentication

Implementing WEP authentication (shared key authentication) on both the AP and the wireless clients had no significant effect on the response time (p = 0.0654) and throughput (p = 0.0655) of FTP, as indicated in *Pair 2* in Table 7-6. However, the

HTTP traffic experienced a slight increase in response time (p = 0.0066) and a drop in throughput (p = 0.0075) of around 7.5%, respectively.

These results indicate that a request-reply message exchange format requires more frequent use of WEP authentication.

7.4.2.3 Impact of 802.1X Authentication Methods

Deploying the 802.1X authentication methods require a RADIUS server and AP support as a RADIUS client. *Pair 4* (see Table 7-6) examined the implementation of EAP-MD5 against the WEP authentication; the authentication method imposed a very significant delay in the network for FTP of 130.6%, or 11.633 seconds (p = 0.0000). The HTTP response time also showed a smaller performance impact of 38.8%, or 7.587 seconds (p = 0.0000). The FTP throughput was reduced by 56.5%, while throughput of HTTP was reduced by 28%.

Pair 7 in Table 7-6 evaluated the different authentication methods used by the 802.1X standard. Using the EAP-TLS authentication significantly increased both FTP and HTTP response times by 3.434 seconds (16.7%) and 1.511 seconds (6.1%), respectively. FTP and HTTP throughputs provided similar results, reducing throughput by 9.5% and 5.4%, respectively.

These results indicate that when incorporating AAA architecture into the network, extra overheads are created, as more authentication frames are transferred over the wireless network. These authentication frames impose significant performance degradation. A large increase in response time and decreased throughputs is experienced when changing basic WEP authentication to more complicated authentication methods. Using certificates instead of username/password methods also introduces another layer of performance overheads, as the EAP-TLS technique requires mutual authentication and provides better key management.

7.4.2.4 Impact of WEP Encryption

The addition of WEP encryption had no significant effect on the response time and throughput of FTP, as indicated in *Pair 3* in Table 7-6. However, encryption caused a decrease of 4.32% in the response time (p = 0.0352) and a slight increase in throughput of 5.26% (p = 0.0202) in HTTP.

Pairs 8 and *9* in Table 7-6 evaluated the effect of WEP encryption when using different authentication methods (EAP-MD5 and EAP-TLS). FTP response time was increased by 93.5%, or 19.207 seconds, while HTTP produced delays of 90.1%, or 22.224 seconds. Both FTP and HTTP throughputs were decreased, by 47.9% and 45.1%, respectively. For *Pair 9*, deploying encryption on top of the EAP-TLS authentication increased FTP response time of 79.6% (18.226 seconds) and HTTP's by 82.2% (21.258 seconds). The throughput for both FTP and HTTP dropped roughly the same amount, by 44.4% and 43.7%, respectively.

These results show that encrypting traffic using WEP causes different results depending on the type of authentication method used in conjunction with WEP. If encryption is used with WEP, there is no burden created on the network for HTTP traffic result (But depends on the key sizes, see Section 7.2.2.5 for key lengths). However, if 802.1X authentication methods are used, a greater impact is experienced. Adding encryption with certificates imposes a longer response time, as per-session keys are generated and transferred from the RADIUS server to the AP. Also the AP wraps the key into a package, introducing more overheads. Request-reply traffic is degraded, as its messages require more processing.

7.4.2.5 Impact of Key Lengths

Pair 5 (see Table 7-6) compared the differences between key lengths of 40-bit and 128-bit used by the WEP protocol. FTP transmissions were significantly delayed, by an additional 1.781 seconds, or 19.78% ($p = 0.0000$). Using a longer key length created a drop in FTP throughput of 16.62% ($p = 0.0000$). No significant effect was found in HTTP response time and throughput.

These results show that as the key length increases, bulk file transfers exhibit significant differences in performance because packets are encrypted and decrypted with a longer key.

7.4.2.6 Integrated Authentication and Encryption Effect

The addition of WEP encryption had a significant affect on overall FTP and HTTP traffic between different authentication methods. *Pair 6* in Table 7-6 examined the performance impacts of WEP and EAP-MD5 authentication methods with encryption, which demonstrated a dramatic increase in response time of FTP by 268.6%, or 28.968

seconds (p = 0.0000). The HTTP response times exhibited similar behaviour, with a 157.3% delay, or 29.811 seconds. Throughputs for both traffic types dropped, by 72.7% for FTP and by 62.4% for HTTP.

Pair 10 tested the effects of using different 802.1X authentication methods with WEP encryption. A slight increase in response time of 3.5% (or 1.384 seconds) was experienced by FTP, while HTTP showed no significant change. Small reductions in throughput were experienced by FTP and HTTP, at 3.4% and 3.0%, respectively.

These results indicate that encrypting traffic poses a substantially greater burden on a network depending on the type of authentication methods deployed. A jump from authentication to incorporating encryption creates additional performance overheads and greater latency when using 802.1X-based authentications. Within the 802.1X authentication range, however, certificates generate only a slight impact on network performance.

7.4.3 Security Mechanisms of the VPN Model

Following the rejection of our null hypothesis that there were no performance differences caused by security levels, we further investigated the impacts and interaction of each security level in the VPN model. The mean level and standard deviation of response time and throughput observed on each security level are given in Table 7-8, while Table 7-9 presents the overview of different paired t-tests. For more detail on the security level information see Table 5-3 in Chapter 5.

VPN Model	Response Time				Throughput			
Security Level	FTP		HTTP		FTP		HTTP	
	Mean	*Std. Dev.*	*Mean*	*Std. Dev.*	*Mean*	*Std. Dev.*	*Mean*	*Std. Dev.*
1. No Security	9.618	0.686	16.721	1.136	117890.65	8348.549	25487.72	1730.131
2. PPTP+CHAP	33.203	0.975	36.448	4.213	35624.95	996.544	13055.80	1412.334
3. IPSec+CHAP	34.440	0.523	39.216	1.709	35462.77	634.893	12788.32	513.672
4. FW+PPTP+CH	25.980	2.752	30.489	1.869	46169.94	4704.064	15222.38	876.847
5. FW+IPSec+CH	25.279	1.999	32.219	2.480	48980.74	3818.477	15251.68	1164.802
6. IPSec+TLS	31.221	2.765	39.022	2.015	39849.83	3400.824	12669.40	626.497
7. IPSec+CH+DES	59.268	4.748	74.121	2.357	21072.77	1691.461	6747.00	225.149
8. IPSec+TLS+DES	86.227	3.115	88.844	2.224	14471.88	510.871	5702.64	178.577
9. IPSec+CH+3DES	64.082	2.341	64.169	3.345	19416.39	651.325	7823.25	423.599
10. IPSec+TLS+3DES	87.000	4.345	88.259	6.067	14422.30	840.074	5792.08	388.031

Table 7-8 VPN Model Descriptive Statistics

As we noted in Section 7.4.2, the following paired t-tests are selected in Table 7-9 were based on the mutual exclusivity[22] of certain security levels and the hierarchical nature[23] of the model. The *Pair* numbers indicate the test comparison of two security levels. Explanations for the following 11 pairs are:

- Pair 1 – compares the difference between no security protection and PPTP tunnelling with CHAP authentication.
- Pair 2 – compares different tunnelling technologies, PPTP and IPSec, using the same authentication method.
- Pair 3 – measures the impact of implementing a firewall onto PPTP-based VPN.
- Pair 4 – measures the impact of introducing a firewall onto IPSec-based VPN.
- Pair 5 – compares different user authentication methods (CHAP and EAP-TLS) used on top of IPSec technology.
- Pair 6 – evaluates the impact of adding the DES encryption algorithm onto CHAP authentication.
- Pair 7 – compares the impact of using DES encryption with EAP-TLS authentication.
- Pair 8 – compares different authentication methods, CHAP and EAP-TLS, when both deploy the DES encryption.
- Pair 9 – compares the impact of different encryption mechanisms (DES and 3DES) based on CHAP authentication.
- Pair 10 – compares the impact of different encryption mechanisms based on EAP-TLS authentication.
- Pair 11 – compares different authentication methods, CHAP and EAP-TLS, when both deploy 3DES encryption.

VPN Model		Response Time				Throughput			
	Security	FTP		HTTP		FTP		HTTP	
Pair	Levels	*t-stats*	*p-value**	*t-stats*	*p-value**	*t-stats*	*p-value**	*t-stats*	*p-value**
1. No Sec vs PPTP	**1 vs 2**	-80.8160	*0.0000*	-14.5848	*0.0000*	32.5071	*0.0000*	18.4451	*0.0000*
2. PPTP vs IPSec	**2 vs 3**	-3.8095	*0.0021*	-2.0804	*0.0336*	0.4575	0.3291	0.6128	0.2776
3. PPTP for FW	**2 vs 4**	7.6081	*0.0000*	4.4003	*0.0009*	-6.9174	*0.0000*	-4.5302	*0.0007*
4. IPSec for FW	**3 vs 5**	14.8094	*0.0000*	6.4247	*0.0001*	-11.4177	*0.0000*	-5.4200	*0.0002*
5. IPSec CHAP vs TLS A.	**5 vs 6**	-8.4820	*0.0000*	-5.1926	*0.0003*	8.6541	*0.0000*	4.9297	*0.0004*
6. IPSec CHAP for DES	**5 vs 7**	-18.2762	*0.0000*	-37.4617	*0.0000*	18.4612	*0.0000*	22.1177	*0.0000*
7. IPSec TLS for DES	**6 vs 8**	-44.7812	*0.0000*	-52.1968	*0.0000*	23.7330	*0.0000*	33.8450	*0.0000*
8. CHAP vs TLS for DES	**7 vs 8**	-15.0010	*0.0000*	-11.5508	*0.0000*	11.6590	*0.0000*	9.6595	*0.0000*
9. CHAP DES vs 3DES	**7 vs 9**	-2.7838	*0.0106*	7.4969	*0.0000*	2.7276	*0.0117*	-7.0237	*0.0000*
10. TLS DES vs 3DES	**8 vs 10**	-0.4863	0.3192	0.2559	0.4019	0.1617	0.4375	-0.5875	0.2857
11. CHAP vs TLS for 3DES	**9 vs 10**	-14.4553	*0.0000*	-13.0008	*0.0000*	14.7083	*0.0000*	12.5331	*0.0000*

*One-tailed at a = 0.05

Table 7-9 VPN Security Performance Comparisons

[22] For example, when users choose security level 7 they cannot have security level 8.
[23] The higher the security level the stronger the protection.

The *Pair* ordering for the t-test comparisons in Table 7-9 were based on the level of security protection from the lowest protection level (1) to the highest (10). The following analysis were also categorised on the level of security quality, thus some of the *Pair* numbers would not be in order in certain sections. The percentage change calculated for each *Pair* comparison was based on Table 7-8's mean values.

7.4.3.1 Impact of Authenticated Tunnels

When the server and clients were configured to create authenticated tunnels, the response times and throughputs changed significantly. In *Pair 1*, FTP response time more than doubled, affecting network performance an increase of 245.2%, or 23.58 seconds. HTTP traffic experienced significant delay over the tunnel of 118%, or 19.726 seconds. Throughput decreases varied; throughput of FTP dropped 70% and HTTP throughput decreased 48.8%.

Pair 2 analysed the performance differences between tunnel protocol types. Only response times showed significant differences, with FTP response time increasing by 3.7% (1.237 seconds) and HTTP by 7.6% (2.768 seconds).

The effect of encapsulating and decapsulating traffic as well as verifying checksums in order to sustain an authenticated tunnel created a substantial cost, causing the level of response time and throughput to change substantially. In addition, different types of tunnelling protocol imposed a slight delay on FTP traffic.

7.4.3.2 Impact of Firewalls

The introduction of firewalls to the VPN improved the response time for FTP by 21.8%, or 7.223 seconds in *Pair 3*. It examined the differences between PPTP with and without a firewall, and HTTP also exhibited a significance difference, response time improved by 16.3% (5.959 seconds). Throughputs increased by 29.6% and 16.6% for FTP and HTTP, respectively.

Pair 4 tested the performance differences between IPSec with and without a firewall, and significant differences were found. Response times decreased by 17.8 % (6.998 seconds) for FTP, and 26.6% (9.161 seconds) for HTTP. FTP traffic experienced a significant increase in throughput by 38.1%, while HTTP throughput increased by 19.3%.

Implementing a firewall decreases response times and increases throughput. These results do not follow the normal assumption of implementation of firewalls: that network performance is degraded because there are extra checkpoints filtering network traffics. See Section 7.5.2.2 for a detailed discussion.

7.4.3.3 Impact of User Authentication Methods

User authentication type was reconfigured at the client to test the effect of using different methods. *Pair 5* tested CHAP and EAL-TLS authentications and showed significant differences in response time and throughput for FTP and HTTP. There were increases in response times of 5.942 seconds (23.5%) for FTP and 6.804 seconds (21.1%) for HTTP. Throughputs for FTP and HTTP decreased at approximately the same rate (18.6% and 16.9%, respectively).

Using certificate-based authentication generates more latency and reduces network throughput more than a simple username/password method.

7.4.3.4 Impact of Encryption

Adding DES encryption caused significant increases in response time for both FTP and HTTP transfers. *Pair 6* tested adding DES encryption with CHAP authentication, and the response times for both FTP and HTTP were increased by 134.5% (33.987 seconds) and 130.1% (41.902 seconds), respectively, their throughputs reduced by half (57.0% for FTP and 55.7% for HTTP).

Pair 7 tested adding DES to the EAP-TLS authentication. Similar results were found to *Pair 6*, the response times for FTP and HTTP decreased by 176.2% (55.006 seconds) and 127.7% (49.821 seconds), respectively. As for the throughputs, FTP experienced a 63.7% drop, while HTTP dropped approximately the same rate as the *Pair 6* analysis, at 55.0%.

Reconfiguring the encryption algorithm to 3DES also produced significant changes. *Pair 9* and *Pair 10* tested adding the 3DES encryption algorithm. *Pair 9* showed that configuring CHAP authentication with 3DES encryption increased the FTP delay slightly by 8.1% (4.815 seconds). However, HTTP response time was decreased by 13.4% (9.952 seconds). The choice of encryption algorithm had smaller impacts on throughputs, reducing it by 7.9% for FTP, but increasing HTTP throughput by 16%.

However, results from *Pair 10* showed that the encryption algorithm used did not have any significant effect on the response times and throughputs for FTP and HTTP.

Encrypting traffic posed a substantially greater burden than merely tunnelling it, although the effect of tunnelling is mostly wasted without encryption. The decision of which cryptographic methods to deploy had a definite performance degradation on FTP traffic, but improvement on HTTP transfers. The type of user authentication chosen were also a factor when it interacted with the encryption algorithm; when using digital certificates, there were no performance differences between the encryption methods chosen.

7.4.3.5 Integrated Authentication and Encryption Effect

Pair 8 and *Pair 11* evaluated the interaction of different authentication methods with different levels of encryption algorithm. Using different authentication methods with the same encryption technique produced significant changes in response time for FTP, with a noticeable increase of 45.5% (26.959 seconds), and an increase of 19.9% (14.723 seconds) for HTTP. Throughputs were reduced by 31.3% for FTP and 15.5% for HTTP.

Pair 11 compared the differences between two authentication systems for 3DES, and significant impacts were observed by FTP and HTTP. Response times for FTP imposed an additional delay of 35.8% (22.917 seconds), and for HTTP a 37.5% delay (24.09 seconds). Throughputs for both types dropped approximately the same percentage of 26%.

The interaction of different authentication and encryption methods produced significant impacts on performance. If the same encryption method is deployed, then the choice of user authentication creates substantial performance overheads and longer response times regardless of which encryption algorithm is used.

7.5 Discussion

As the security level gets higher, the general trend is increased response times and decreased throughputs. The charts from Figures 7-3 to 7-6 present overviews of the security mechanisms' impacts on performance. The 802.1X model provides better response times and throughputs than the VPN model; the IPSec-based VPN model provides end-to-end security that produces more performance overheads. We found that

FTP performed better than HTTP, because the nature of their transmission is different and means that HTTP requires more interaction between the server and the client. However, during the security level analysis (Section 7.4), some security mechanism impacted FTP transactions more than the HTTP[24]. Providing same data file sizes for both traffic types would represent a better measurement for HTTP.

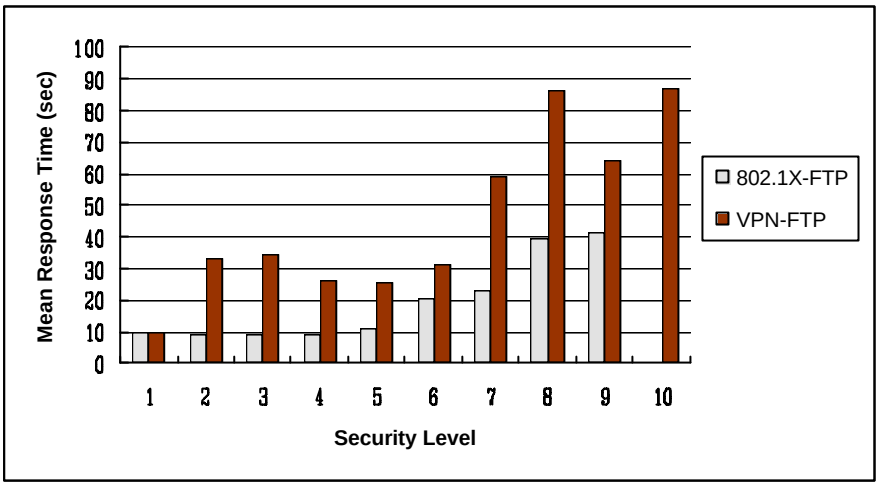

Figure 7-3 FTP Mean Response Times of the Two Models' Security Levels

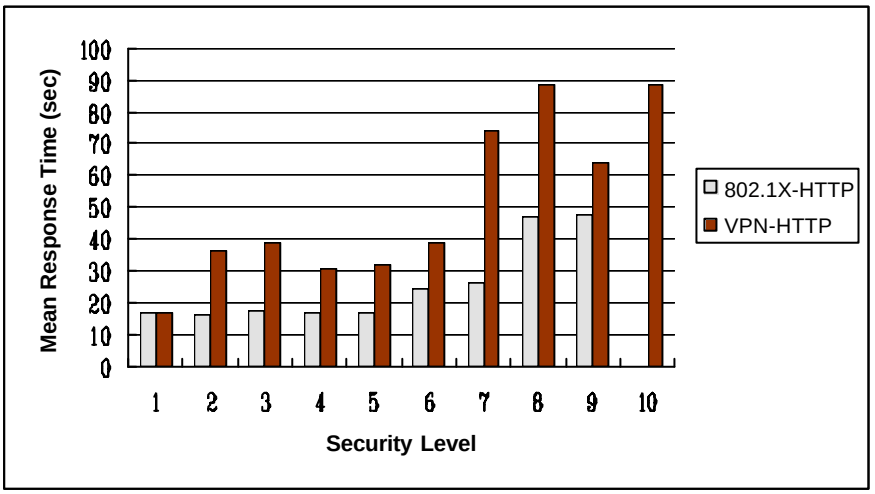

Figure 7-4 HTTP Mean Response Times of Two Models' Security Levels

Inverse relationship was found in both 802.1X and VPN models between response time and throughput: as response time increased throughput decreased. See Figures 7-3 and 7-5 for FTP traffic and Figures 7-4 and 7-6 for HTTP traffic.

[24] For example, when choosing EAP-MD5 authentication in the 802.1X over WEP authentication, the HTTP was less impacted on response time and throughput.

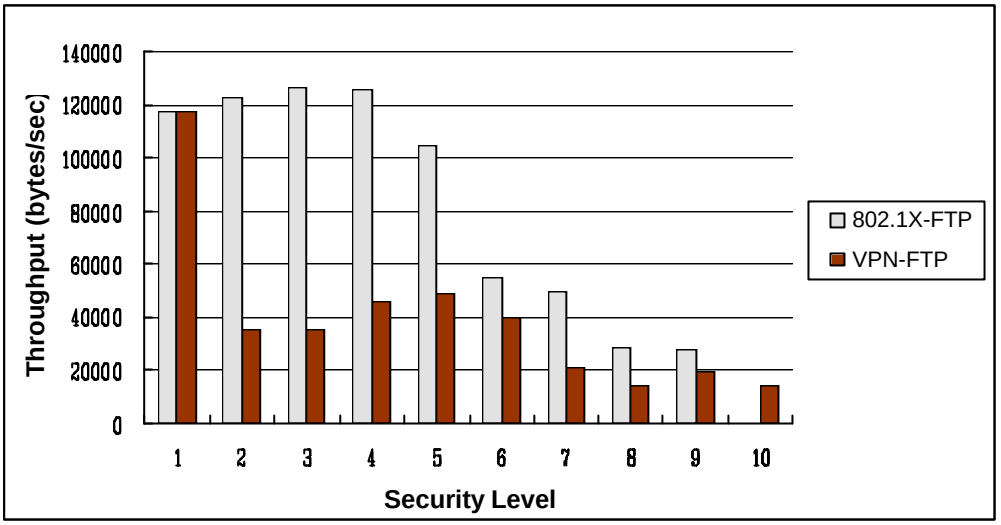

Figure 7-5 FTP Mean Throughputs of Two Models' Security Levels

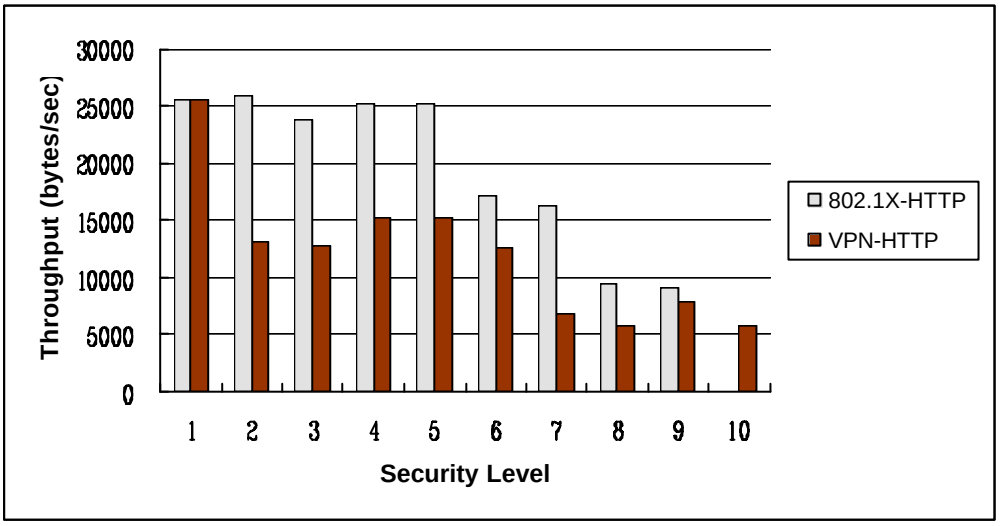

Figure 7-6 HTTP Mean Throughputs of Two Models' Security Levels

7.5.1 802.1X Model

Deploying the 802.1X infrastructure causes increased performance degradation compared to the 802.11 standard.

7.5.1.1 Authentication

MAC address authentication produces no performance overheads when compared to the default security setting, and thus should be used at all times. The 802.11 standard's WEP (shared key) authentication creates a positive effect on FTP throughput but decreased HTTP throughput by 7.5%. Since the effect is small, WEP authentication should be deployed.

The result of deploying AAA architecture imposes significant performance degradation. Using 802.1X authentications methods degraded network performance significantly compared to WEP authentication. Furthermore, EAP-TLS produced more performance impacts than EAP-MD5, as it provides mutual authentication and key management.

7.5.1.2 Encryption

WEP encryption improved the network performance slightly, at approximately 5% in HTTP. However, different longer key lengths 128 bits impacted FTP performance less than 20%. Depending on the nature of traffic transmission, the strongest key length should be deployed.

When adding WEP encryption onto 802.1X authentications, more specifically, EAP-MD5, dramatic degradations are experienced with 100% increases in response times and 50% decreases in throughputs for both traffic types. Certificate-based authentication with WEP encryption provided similar results.

7.5.1.3 Interaction between Authentication and Encryption

When comparing the combined effect of authentication methods and encryption, the overall degradation was severe. For FTP, the response time increased by more than 268% and throughput reduced by 73%. HTTP experienced similar results at a smaller rate. These results indicate that encrypting traffic poses a substantially greater burden, but depending on the type of authentication method deployed. Between EAP-MD5 and EAP-TLS, the performance impact was minimal, at approximately 3%.

7.5.2 VPN Model

Implementing a VPN model provided stronger protection with complex cryptographic methods, and better key management.

7.5.2.1 Tunnelling

An authenticated tunnel created a dramatic response time delay of more than 245% for FTP and 113% for HTTP. Throughputs were reduced by more than 50%. The latency was greater than Rodgers' finding of 85%, but his study did not observed any impact on throughput. This may be due to the transaction size or the transmission medium differences. Different tunnelling technologies impacted only the response time of the traffic; with HTTP traffic affected slightly. Certificate-based authentication (EAP-TLS) generated more than 20% delay and reduced throughput by 17% for all traffic types.

7.5.2.2 Firewalls

Implementing a firewall actually improved the network performance by more than 15% regardless of which tunnelling protocol was used. This finding contrasts with the observation made in Rodgers' [2001] study that firewalls degrade network performance by more than 30%. The difference between our research and Rodger's were due to (1) software and hardware firewall, and (2) end-to-endpoints and between security gateways. IPSec protection was provided by the hardware firewall in Rodgers' research, while we provided the protection at endpoints.

Since the number of packets before and after the firewall implementations are roughly the same, the only factor altered was the response time. One possible explanation could be that the software firewall and router reside on the same Windows machine causing side effects that produce positive results on network performance (for example, interactions between the firewall software and the TCP/IP stack). The software firewall would probably intercept messages and process them before the rest of the operating system gets them. This means that optimisation concerning buffering and open connections could increase the speed of connections. Further investigation could include running the firewall on a separate machine to test the outcome.

7.5.2.3 Encryption

Encryption poses a substantially greater burden than merely tunnelling the traffic. Certain cryptographic methods produced definite performance degradation on FTP traffic, but HTTP performance improved. Deploying DES encryption created more than a 130% delay and 50% reduction in throughput for CHAP and EAP-TLS authentication methods. For stronger encryption only FTP traffic was degraded regardless of the user authentication methods was used. Mixed results were found on traffic response time, with 8.1% increase for FTP and 13.4% improvement for HTTP accompanying CHAP authentication. FTP throughput decreased by 7.9%, and HTTP throughput improved by 16%. The type of user authentication chosen also played a role when interacting with the encryption algorithm; when using digital certificates, there was no difference between encryption methods chosen.

7.5.2.4 Interaction of Authentication and Encryption

Combing different authentication methods with encryption produced significant impacts on performance. If same encryption method is deployed, e.g. DES, then the choice of

user authentication methods created substantial performance overheads and longer response times regardless of the encryption algorithm used. For DES, FTP is affected more than double the HTTP amount at a 35.8 % delay and 31.3 % drop in throughput. But for 3DES, using CHAP or EAP-TLS authentication produced similar effects.

7.5.3 Overall Performance

These results are limited to a single cell WLAN. Integrating these models with a backbone network would provide further information on different traffic loads transferred over the network.

The two measured indicators of performance, throughput and response time were affected by the security mechanisms deployed. We can generalise our findings in the following points (for more details, see Table 7-10):

- Deploying MAC and WEP authentication created no overheads.
- Different authentication methods created different levels of performance overhead; EAP-TLS generated the longest delay and decreased throughput. A comparison of the authentication mechanisms can be summarised as follows:
  - ✓ EAP-TLS> EAP-MD5/CHAP>WEP>MAC
- Tunnelling produced large overheads; IPSec overheads > PPTP overheads.
- WEP encryption impact on performance varied; key length affected only response times. However, when WEP encryption was used in conjunction with 802.1X-based authentication, network performance was dramatically degraded.
- Deploying DES cryptographic methods introduced large overheads, however, there was not much difference between 3DES and DES, especially when used with a certificate-based authentication.
- The interaction of authentication and encryption generated different results from adding encryption to the same authentication methods for FTP and HTTP traffic. EAP-TLS produced the most adverse impact.
- Firewall deployment (router integrated) provided some interesting results. Performance was actually improved instead of degraded. Further investigation is required.

Security Impact on Performance (significant % change)	802.1X Model				VPN Model			
	Res. Time		Throughput		Res. Time		Throughput	
	FTP	HTTP	FTP	HTTP	FTP	HTTP	FTP	HTTP
Authentication								
- MAC	0	0	0	0				
- WEP	0	<10	0	<10				
- EAP-MD5 > WEP	>100	<50	50-100	50<				
-EAP-TLS > MD5/CHAP	<50	<10	<10	<10	<50	<50	<50	<50
Tunneling								
-PPTP					> 100	>100	50-100	<50
-IPSec > PPTP					<10	<10	0	0
Firewall								
- PPTP					Imp	Imp	Imp	Imp
- IPSec					Imp	Imp	Imp	Imp
Encryption								
-WEP (40-bit)	0	Imp.	0	Imp.				
-WEP 40-bit vs 128-bit	<50	0	<50	0				
-EAP-MD5 with WEP	100<	100<	<50	<50				
- EAP-TLS with WEP	100<	100<	<50	<50				
-CHAP with DES					> 100	>100	50-100	100-100
-TLS with DES					> 100	>100	50-100	50-100
-3DES> DES with CHAP					<10	Imp	<10	Imp.
-3DES> DES with TLS					0	0	0	0
Integrated Authentication & Encryption								
- WEP vs MD5 with WEP	>100	>100	50-100	50-100				
-TLS-WEP vs MD5 WEP	<10	0	<10	<10				
- TLS > CHAP with DES					<50	<50	<50	<50
- TLS > CHAP with 3DES					<50	<50	<50	<50
Imp = improve the network performance								

Table 7-10 Summary of Security Impact on Performance

7.6 Summary

Our experimental evaluation investigated the performance cost incurred with various security mechanisms, and found that the more secured a network became, the higher the performance impacted. The VPN model incurred more performance degradation than the 802.1X model as we expected; the VPN model provided end-to-end security with double authentication (device and user), stronger encryption method, better key management, and tunnelling technology. The general pattern for type of application protocols carried over a network also followed our expectation that request-reply (HTTP) application created more performance overheads than the FTP, as the

interaction between two endpoints increased due to security negotiation and management. Our evaluation on different security levels showed that the higher the security level got (as the network became more secured), the greater the performance cost generated, except in the case of MAC address authentication, WEP authentication and encryption (40-bit), a firewall, and 3DES encryption in the VPN model. Further research would be required on investigating software or hardware firewall's effect on the network, and different traffic characteristics for different cryptographic methods.

CHAPTER 8

Wireless Security Insurance

Arbaugh [Goth, 2002] provided the insight on security that "the biggest problem with security is management: how to do it well, how to do it consistently, and how to make it easy on your IT staff. It is not the underpinning of cryptography, not deciding to run security at layer 2 or layer 3, but how do you manage all of this?" Our experimental results quantified the security impact on performance; however, to maintain a secured wireless network, security management strategies must be constructed and enforced. In this chapter, we propose a novel way to evaluate security as "insurance policies" (see Section 4.4), thus creating a positive cycle for enforcing standard security practices. The performance impact results from our experiments act as one of the insurance policy variables in assessing network security.

When organisations plan network security strategies, their particular organisational environments determine the security mechanism or combination of mechanisms they will choose. Security policies can be written like insurance policies, and various factors include company size, value of assets, priority of security, and performance cost. This chapter illustrates how insurance policies could be constructed in terms of performance overheads. Various scenarios demonstrate how security insurance policies can be applied to organisations deploying wireless networks.

8.1 Scope of the Security Insurance Concept

Providing security insurance can generate business opportunities. Organisations mitigate risk at a level that insurance companies find acceptable. Insurance companies evaluate the value of a company's assets to be protected and the residual value of risk. Security insurance policies will be based on the insurance companies' assessments and evaluation, and sufficient to cover the network security risk. Following this concept, active security monitoring and management is required, which further strengthen a company's network security against threats and attacks.

The security insurance framework to be established will contain various factors, including the value of a company's assets, a company's reputation, company size, security, the performance cost, end-user characteristics (level of IT knowledge, behaviour[25] etc.), and existing network resources (software and hardware) that have been deployed by a company. Insurance companies will assess these requirements to provide security insurance to organisations. A security insurance evaluation process is described in Figure 8-1. The proposed wireless security insurance strategies in this study investigated only two components, security policies and performance cost. Other components were beyond the scope of this study.

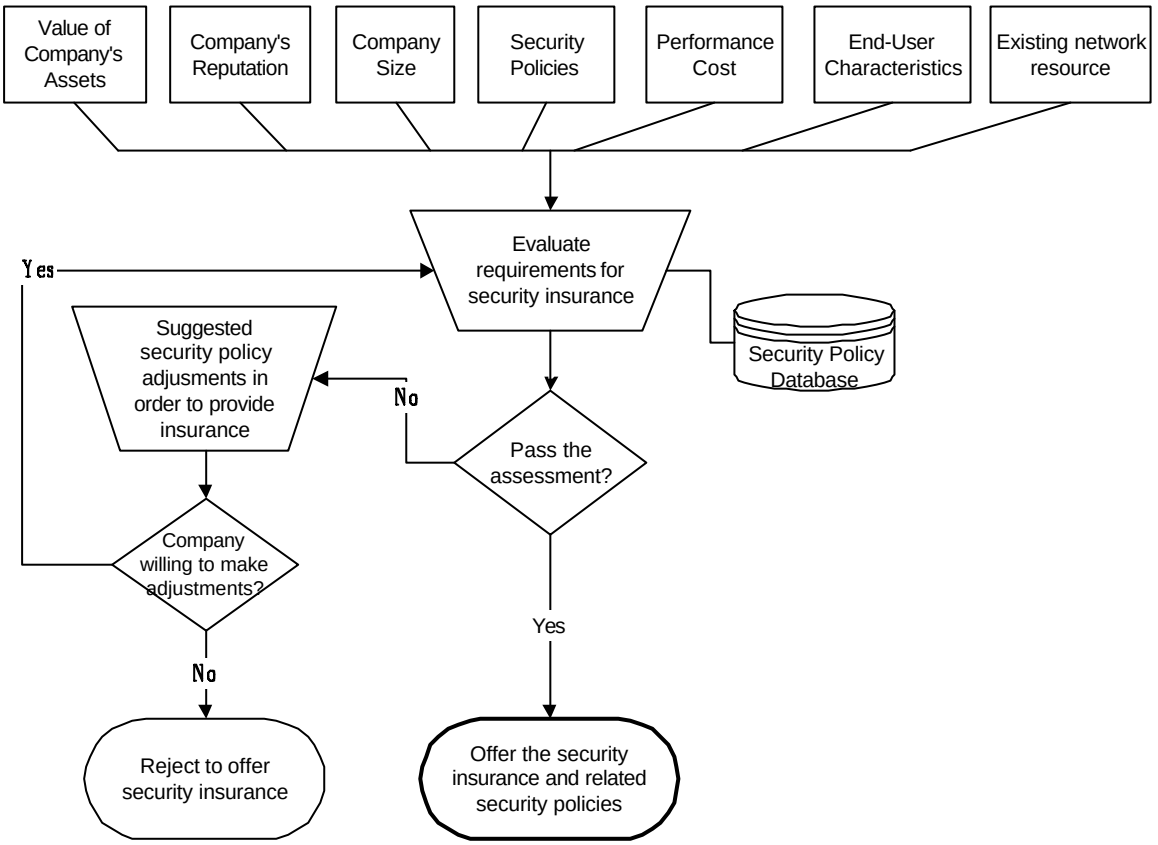

Figure 8-1 Security Insurance Evaluation Process

8.2 Wireless Security Policies

There are several factors that would be necessary to issue security insurance. The factors defined in this section were chosen to provide a template for wireless security polices. Table 8-1 provides a WLAN security policy template. The template represents various security policies that can be implemented for an organisation's WLAN networks. Factors considered in the template include:

[25] If end-users tend to abuse of a company's information resources, a higher premium may be required.

- *Policy number:* provides an index number for ordering the policies.
- *Protection type:* provides information on which policy belong to what risk mitigation. This is generalised from Section 3.3 and Chapter 5. There are three types of protection provided in the template: basic, 802.1X and VPN models. Policy numbers 1 to 6 are the default policies, which must be deployed regardless of type of security.
- *Security priority of the policy:* states the quality of security offered by each policy. The priority ranges from level 1 (lowest) to level 3 (highest). The higher the security priority levels are associated with stronger protection.
- *Policy description*: details the content of the security policy. These descriptions are based on the risk countermeasures discussed in Chapter 3 and our security levels for the 802.1X and the VPN models defined in Chapter 5.
- *Performance cost:* that is associated with each policy. The performance cost is calculated in terms of a percentage of throughputs; this number is based on the average throughput associated with FTP and HTTP, as evaluated in Section 7.4. If certain security policies are more time sensitive, they will be indicated by symbols in the template. Some security policies require other policies to be activated in order for them to work, thus, letter "P" indicate which policy number needs to be incorporated when calculating performance degradation.

This template provides only a limited view, as the parameters considered in this research concentrated on security techniques and performance. Other parameters such as value of a company's assets, end-user characteristics, and multiple WLANs have not been evaluated. Note that firewalls are not included in the 802.1X and VPN model protection types, but are included in the basic protection type.

Policy No.	Protection Type	Security Priority	Policy Description	Perf. Cost (%)
1	Basic Protection	1	Change default passwords for accessing access points.	0
2		1	Change access points' SSIDs so that they do not reflect obvious names, e.g. function of an AP, but a mixture of departments, division, or organisational policy.	0
3		1	Physical protection of APs and wireless NIC cards by keeping an inventory list.	0
4		1	Change or disable SNMP parameters and other non-essential management functions.	0
5		1	Change and deploy channel settings to ensure minimum interferences.	0
6		1	Update wireless devices with the latest patches to ensure device integrity.	0
7		1	Deploy DHCP if the network has a large number of users or a public network.	0
8		2	Install a properly configured firewall between the wired and wireless networks.	-25?
9	802.1X Model Protection	1	Deploy MAC address authentication.	0
10		1	Enable WEP authentications.	0
11		1	Deploy WEP encryption with 40-bit key length.	-2.6
12		2	Deploy WEP encryption with 128-bit key length.	8.3
13		2	Implement 802.1X framework with EAP-MD5 authentication method.	42.3†
14		3	Implement 802.1X framework with EAP-TLS authentication. EAP-TLS is based on PKI technology and provides enhanced key management.	7.5 + P13
15		2	Deploy WEP encryption with 802.1X authentication method EAP-MD5.	46.5F
16		3	Deploy WEP encryption with 802.1X authentication method EAP-TLS.	45.8?
17	VPN Model Protection	2	Deploy PPTP tunnelling with CHAP authentication for a Layer 2 VPN.	59.4F
18		2	Deploy L2TP/IPSec tunnelling with CHAP authentication.	P17
19		3	Deploy L2TP/IPSec tunnelling with EAP-TLS authentication.	17.8 + P18
20		3	Adding DES encryption onto IPSec-based VPN with CHAP user authentication.	56.4F
21		3	Adding DES encryption onto IPSec-based VPN with EAP-TLS user authentication.	59.4F
22		3	Adding 3DES encryption onto IPSec-based VPN with CHAP user authentication.	4.1+ P20
23		3	Adding 3DES encryption onto IPSec-based VPN with EAP-TLS user authentication.	P21

? - normal firewall considerations apply; the cost is specific to this research using a software firewall/router.
† - If the nature of traffic is FTP, a more severe impact is experienced.
? - if the nature of traffic is HTTP, a more severe impact is experienced.
F - time sensitive impact as well.
P - the policy number (and its associated cost).

Table 8-1 A Wireless Security Policy Template

8.3 Scenarios

The following scenarios are examples of how the wireless security policies described in Table 8-1 could work if insurance companies consider providing IT security insurance for WLANs. The company sizes are selected from Section 4.3. Some of the network performance degradation may seem large, however note that network performance

degradation is just one of the variables in evaluating the security insurance requirements.

To maintain a company's network performance at the base level (before applying the security mechanisms), there is a cost to the company, such as the cost of upgrading equipment (servers, workstations), faster network (upgrading to 802.11a), and so on. These costs are in addition to the direct cost of purchasing the security tools, which includes hardware, software, and the staff to maintain and enforce the security implemented on the network.

8.3.1 Small Company

ABC is a small retailing company and has a small WLAN in place. The owner currently has no security protection mechanism in place. After evaluating the value of the company's assets protected by the network security, the insurance company required the owner to apply the following security policies:

- Basic protection type (policy numbers 1 to 6) as these policies are used for basic security management. No performance degradation will be experienced. No DHCP policy is required, as the company's size is small.
- 802.1X model protection (policy numbers 9-10, and 12), which provides MAC address, and WEP authentication and encryption (128-bit). The network performance throughput would be decreased by 5.7 %. As the company's asset value does not require strong security mechanisms, basic defence tools such as MAC address and WEP protection are sufficient.
- The overall performance degradation is 5.7 %. No additional security tools that must be purchased, because MAC addresses and WEP protection can be activated in the AP[26]. User training would be minimal, and maintenance costs are small, but would require a part-time staff to keep updated MAC addresses and software patches.

8.3.2 Medium Company

IJK is a medium-sized hardware manufacturer, and has deployed a few APs in the factory. Product designs and other valuable information are usually transmitted over the air. The company has consulted with an insurance company on mitigating their risks

[26] If the APs currently deployed do not provide these mechanisms, the company should consider purchasing high-end wireless products if the cost of buying these products justifies the security protection.

against attacks. After its evaluation, the insurance company suggested the following policies:

- Basic protection type (policy numbers 1 to 8), DHCP is required to provide easier IP address issuing. A firewall must be placed at the edge of the company's core network, separating wired and wireless networks. The network performance impact might result in a 25% increased in throughput (see Table 8-1).
- 802.1X model protection type (policy numbers 9, 14, and 15) to provide MAC address authentication, and EAP-TLS authentication with WEP encryption. MAC address authentication is used on wireless devices, and EAP-TLS for user certificates. The network performance degradation that would be experienced is 95.6%. PKI is selected because company data is valuable, and certificates provide better access control than EAP-MD5.
- The overall performance impact on the network is a decrease of 70.6%. IT staff need to be trained in operating the company's own certificate and RADIUS servers, and applying remote access policies. Outsourcing a certificate server provider may be considered, such as VeriSign[27], if the company is considering e-commerce for the future and the subscription fee justifies its use. User learning curves would not be high as digital certificates, once installed, provide automatic sign-in.
- The VPN Model was not recommended as creating tunnels generates high performance overheads, which are not efficient in transmitting multimedia data such as product designs.

8.3.3 Large Company

Organisation QRS is a large financial institution, and has deployed several WLANs. Its data transmission must be secured to protect the sensitive documents being transferred across the organisation. It decides to insure the value of its data and asks an insurance company to provide an assessment.

After the assessment, the insurance company proposes the following policies:

- Basic protection type (policy numbers 1-8), because the organisation has a large number of wireless users, DHCP is required to issue IP addresses,

[27] A commercial certificate authority providing public-key infrastructure (PKI) security solutions, see www.verisign.com.

as stated in policy number 7. Furthermore, installing firewalls between departments (policy number 8) is a necessity, which might increase the network throughput by 25%.

- VPN model protection type (policy numbers 19 and 23) deploys IPSec tunnelling with certificate authentication (EAP-TLS) and the strongest encryption method, 3DES. These selections provide the strongest data protection. This would produce network throughput degradation of 136.6%.
- The overall performance impact on the network would be a decrease of 111.6%. User and IT staff training are crucial to ensure an effective use of IPSec technology. Operating IPSec based VPN requires a level of sophistication from IT staff, such as providing tunnelling, and configuring IPSec policies. There is an additional cost of purchasing security products. Outsourcing IT expertise may be considered.

8.4 Summary

The security insurance concept introduced in Chapter 4 has been applied here to WLAN. Our analysis has led us to propose a template for wireless security policies in terms of performance cost. The security policies are treated as a factor in determining insurance requirements with performance cost as one of the premium indicators. Other factors that shape the premium calculation, such as the value of a company's assets and company's reputation, have not been selected as they are beyond our research scope. Various examples in Section 8.2 show how these policies might work to provide better security and generate business opportunities in the industry. Business sectors can use this template as an indicator of their network security and performance tradeoffs, while insurance companies can use such policies to generate new business revenue and strategies.

CHAPTER 9

Conclusions

Our research quantified the tradeoffs between performance and security of 802.11 WLANs. The data show that security mechanisms produce performance overheads in both wired (from prior research) and wireless networks (from our experiments). However, these overheads vary widely, and depend upon the security architectures and their related configuration options.

We defined two AAA-integrated models to secure 802.11b networks. These two models were constructed with various security layers. The 802.1X model includes MAC address authentication, WEP authentication and encryption, and 802.1X EAP-MD5 and EAP-TLS authentication methods. The VPN model is based on IPSec technology, and contains a firewall, tunnelling, PKI device authentication, CHAP and EAP-TLS user authentication, and DES and 3DES encryption algorithms. The FTP and HTTP traffic types were selected to demonstrate the difference between bulk-file and request-reply transfers. The general pattern we found in the experiments was that the stronger the security mechanism implemented, the poorer the network performance. In other words, as the level of security increases, WLAN performance degrades, although such performance penalties varied widely.

9.1 Research Results

The VPN model offered end-to-end security, which was superior to the 802.1X model and doubled the response time and reduced throughput by one-third. However, the level of complexity for security implementation increased when the VPN model was deployed. The visible performance degradation was experienced when the VPN model was deployed using tunnelling, the combined effect of device- and user-authentication, and a stronger encryption algorithm. Unless strong protection is required (such as classified government or military data), organisations should implement the 802.1X model as it offers simpler network management and requires fewer network resources at the network boundary.

The type of traffic used for data transfer influenced the results. A comparison between FTP and HTTP traffic found that HTTP traffic created greater overheads with longer response times than FTP traffic. Due to the nature of the HTTP traffic, the results illustrated our assumption that as the number and size of authentication and management frames increased in interactive applications, users would experience extended delays and decreased throughput.

Our ANOVA analysis confirmed that security levels within each model produced different impacts on performance. Furthermore, most security mechanisms degraded network performance as the quality of the security protection increased. Certificate-based authentication (EAP-TLS) significantly increased response times and decreased throughput more than password-based authentication (EAP-MD5/CHAP). WEP encryption (128-bit) produced a lower impact on a network than the DES or 3DES encryption methods. However, there were a few exceptions observed that produce no significant impact on performance, examples include MAC address authentication, WEP encryption (40-bit), WEP authentication, and 3DES encryption (when compared to DES encryption). Thus, these security mechanisms should be used whenever possible.

Some unexpected results were observed when the software firewall was implemented which, in fact, resulted in improved network performance. Further research is required on the choice of software/hardware security device implementation, and at which point in the network path to provide IPSec protection.

A novel concept of writing up security policies as one of the wireless security insurance requirements, using the size of performance degradation as part of the premium calculation, may provide business and security enhancement incentives. If IT security can be insured, a business has an incentive, if it regards its data as critical or valuable, to deploy the best security it can afford thus minimising its risks and insurance costs. On the other hand, insurance companies will provide insurance if certain security criteria are met. These business opportunities can generate revenues for insurance companies, thus leading them to demand stronger security protection to avoid losses. The wireless security policy template we constructed in Table 8-1 illustrates how these security policies can be used in various scenarios. We proposed security policies and performance degradation cost (impacted by security) as some of the requirements to construct wireless security insurance; other parameters include a company's reputation, the value of company assets, and company size.

9.2 Limitations

IT security requires both human intervention and technical support to provide a secure network solution. This research focused on the technical support for a secured wireless network. The human aspect is equally important but will not be investigated due to the limited timeframe and resources.

This study examined only one type of wireless network, the 802.11 standard; the results of this study might not be applicable to all types of wireless networks. One limitation of this research was the use of the infrastructure mode of the 802.11 standards. This might preclude generalisation of these performance or security results to the ad-hoc mode of 802.11 wireless networks (see Section 2.2.1). We assume that many organisations deploying a WLAN use the infrastructure mode design. Network traffic generated during the experiment is assumed to mimic real world traffic flow.

In general, there are several limitations associated with experiments. Experiments are tested in a confined environment, which may not simulate the real world. Real world factors such as environmental effects are important in wireless networks, because radio frequency transmission is influenced by other technologies operating in the same frequency band, such as microwaves, and weather conditions. These interferences may affect the performance results of a wireless network.

One inherent limitation is using vendor-specific equipment. Different vendors provide different capabilities, and as prior literature has shown [Avery, 2001], different hardware can affect performance.

The experiments conducted had a single-cell design with a single client to server communication route. Therefore, multiple clients or multi-cells design using multiple APs are beyond the scope of this research. By operating with one client, the parameter of network congestion has not been taken into account.

The characteristic of FTP and HTTP application protocols provide different file sizes thus direct comparison will show limited results.

9.3 Future Work

As wireless network access grows, new business opportunities will be created. M-commerce may be the next major enhancement to e-commerce. The advantage of increasing mobility will lead to stronger demand for QoS, and simpler roaming structure at a secured connection.

Our research was limited to a single client and server pair operating in a single cell, and future work could incorporate inter-cell or inter-AP support for single and multiple users. As mobility increases from WLANs to WWANs (handoffs between the two), the ability to maintain a secured connection without reassociation and reauthentication as a user roams from one network to another should be investigated. To further widen the scope, experiments using multimedia data types at various sizes could be conducted.

Future research can explore the security insurance policy concept, such as integrating parameters other than performance cost. An area to be investigated is the interactions between different business models and insurance assessments.

Another area to be investigated is the accounting and billing consideration against security support. Experiments can be carried on the interactions between accounting and security for wireless users accessing secured public WLANs. Deploying a PBNM framework can enhance security as it provides automatic network resource configuration through high-level policies. PBNM may be integrated with a usage-based fee scheme to provide dynamic network auditing and management for a service provider [Geng et al., 2002]. Users will demand higher security, thus leading to better security frameworks supported by service providers.

Appendix A Captured Data

802.1X Model

802.1X Model	FTP		HTTP	
Security Level	Response Time(sec)	Throughput(bytes/sec)	Response Time(sec)	Throughput(bytes/sec)
1	9.5157	118445.8316	17.9688	23685.0541
1	8.9058	126570.6618	16.5044	25642.4347
1	8.7125	129365.6241	17.6590	23888.4988
1	10.1177	111338.3476	14.8066	28488.8496
1	9.0351	124710.0752	17.7286	23860.2033
1	10.3231	109298.3697	15.8741	26655.6214
1	10.5541	106843.0278	18.2818	23328.0640
1	10.4326	108135.46	16.1912	26365.2478
1	9.1216	123522.7372	16.4557	25898.6856
1	9.4628	120676.3326	15.7446	27064.5809
2	9.2861	121288.2696	16.9248	24930.5162
2	9.1525	122974.2693	17.9601	23507.9983
2	9.1567	122917.7542	18.0325	23403.1332
2	9.8041	114901.7248	15.0625	28057.1618
2	8.9462	125871.655	15.4000	27282.7922
2	8.8786	126762.2148	16.2016	26018.1093
2	9.082	123928.7602	16.0104	26188.6024
2	8.5825	131218.6426	16.4815	25589.7825
2	9.9847	112828.4275	16.3508	26058.9084
2	8.8653	127008.1103	15.6499	27204.4550
3	8.4729	133046.0645	17.2726	24414.6799
3	8.1582	138210.3895	17.7482	23710.5171
3	9.4307	119423.3726	17.2118	24797.1159
3	9.0701	124140.3072	18.4000	23100.4348
3	9.0121	124877.8864	17.5556	24056.6543
3	9.0083	125138.2614	19.1260	22226.3411
3	8.6693	129846.8158	18.2387	23176.3777
3	8.8178	127856.7216	17.6838	24151.9357
3	9.3757	120183.7729	16.6827	25487.0614
3	9.0972	123922.1958	17.7616	23753.4344
4	9.6753	116877.3061	18.5498	22881.9179
4	9.1612	123681.6138	17.5314	24538.7134
4	9.4281	119704.1822	18.1697	23390.3146
4	8.1676	138458.9108	16.3412	26138.5333
4	8.8407	127876.1863	15.9270	26690.5883
4	9.5237	118799.6262	16.9590	25213.2201
4	8.2238	136961.7452	17.3283	24574.0205
4	9.3309	120912.8809	16.1179	26313.3535
4	9.5202	118519.5689	16.2067	26069.3417
4	8.15	138222.8221	16.8763	25625.9962
5	12.3404	91505.21863	17.0239	25056.4207
5	9.8204	114694.9208	15.6329	27128.4279
5	10.4053	108362.8535	16.8415	25291.6308
5	9.8873	114084.1281	19.5765	21841.8001
5	11.2831	99860.05619	18.0417	23549.3884
5	10.2715	109747.1645	19.6843	21614.0274
5	11.2999	99906.19386	16.6715	25342.5307
5	11.0485	102272.4352	15.1878	28131.0657
5	11.1828	100676.7536	16.2790	25907.6725
5	10.2872	109483.1441	15.8362	27081.1811
6	21.0347	53819.7835	26.3943	16152.3890
6	21.9662	51363.77708	25.1228	16878.5326
6	20.1928	55811.97258	21.9044	19238.4179
6	21.8685	51532.06667	24.6403	17176.0490
6	21.8971	51438.31832	22.2398	19190.1006
6	18.0979	62423.98289	25.6157	16368.4771
6	19.4996	57773.08252	23.9657	17484.3213
6	21.5198	52421.95559	25.9596	16310.9216
6	20.9949	53657.60256	26.2169	16145.2727
6	18.372	61293.70782	24.5932	17068.6206
7	26.1518	43266.81146	28.6559	14817.4023
7	26.6256	42496.80758	26.2564	16150.0053
7	23.2085	48739.85824	25.3614	16680.0334
7	22.4488	50655.04615	27.4342	15528.0635
7	23.0486	49107.40783	25.8271	16493.1022
7	24.7353	45914.54318	25.6679	16737.5983
7	20.0363	56381.71718	25.3586	16701.5924
7	19.7089	57318.26738	24.7501	17164.3347
7	22.5927	50099.50117	26.2047	16236.6675
7	20.5363	55011.85705	26.2452	16220.2993
8	39.5425	28808.19372	48.2178	9136.7296
8	38.9094	29292.12478	46.1852	9339.5936
8	39.6817	28787.32514	47.2489	9415.4361
8	40.0551	28444.36788	46.7312	9463.2922
8	39.6652	28725.17975	46.5072	9774.2930
8	39.4241	28899.55636	46.6443	9463.8144
8	40.1168	28706.97563	46.6951	9309.9062
8	40.0268	28465.90285	45.3921	9749.2736
8	39.8447	28603.85446	47.5624	9396.9186
8	40.2446	28344.42385	47.7013	9337.4814
9	39.6139	28752.40761	47.1130	9275.1258
9	41.5942	27381.05313	48.0532	9026.5373
9	41.3027	27585.24261	46.4493	9308.4718
9	41.5018	27602.22448	46.0815	9382.4203
9	41.7071	27341.91541	48.4151	8975.8980
9	40.6446	28023.13222	49.1880	8804.1799
9	40.6528	28090.29144	46.9852	9214.5825
9	41.7536	27474.73272	47.0500	9321.6366
9	40.6807	27989.41513	46.1593	9477.1801
9	41.8961	27186.25361	48.8476	8816.5846
Total	1718.2746	7600892.434	2301.3944	1775104.953

VPN Model

VPN Model	FTP		HTTP	
Security Level	Response Time(sec)	Throughput(bytes/sec)	Response Time(sec)	Throughput(bytes/sec)
1	9.5157	118445.8316	17.9688	23685.05409
1	8.9058	126570.6618	16.5044	25642.43474
1	8.7125	129365.6241	17.659	23888.49878
1	10.1177	111338.3476	14.8066	28488.84957
1	9.0351	124710.0752	17.7286	23860.20329
1	10.3231	109298.3697	15.8741	26655.62142
1	10.5541	106843.0278	18.2818	23328.06398
1	10.4326	108135.46	16.1912	26365.24779
1	9.1216	123522.7372	16.4557	25898.68556
1	9.4628	120676.3326	15.7446	27064.58087
2	32.9566	35810.36879	41.6196	11276.99449
2	34.0292	34675.60213	44.0871	10694.64764
2	31.9443	36949.84708	33.3882	14012.76499
2	33.7437	34978.91458	35.1763	13405.04829
2	32.2587	36655.53789	34.8316	13443.22397
2	32.4205	36337.34828	31.9639	14863.61176
2	34.9024	34087.94238	34.7615	13609.28038
2	33.6095	35342.89412	40.7508	11606.96232
2	33.9048	34755.55084	32.0612	14589.2543
2	32.2587	36655.53789	35.8366	13056.20511
3	35.1364	34614.64464	41.4784	12013.67459
3	33.6808	36417.72167	39.5049	12667.31469
3	34.1281	35691.52692	36.3088	13724.469
3	34.4001	35789.51805	38.1705	13028.3596
3	34.8902	34955.11634	38.1073	13103.78851
3	33.9147	36158.50944	38.7725	12831.41402
3	34.5419	35224.09016	38.8785	12957.72728
3	34.5622	35362.65053	38.9407	12837.28849
3	35.1919	34536.95311	42.3333	11955.90705
3	33.9537	35876.97364	39.6657	12763.2186
4	27.8488	44056.58413	27.7058	16557.83266
4	26.2190	45057.6681	31.7598	14599.24181
4	25.7733	46463.16149	32.0520	14442.62449
4	26.8032	44100.66708	30.0023	15309.25962
4	22.2219	53078.49464	28.4715	16136.97908
4	30.4842	38901.72614	30.2165	15471.5801
4	23.3732	50595.81059	30.0207	15427.2885
4	29.5585	39722.82085	32.9519	14147.49984
4	23.6277	50108.85528	28.7687	16062.59581
4	23.8906	49613.61372	32.9370	14068.88909
5	24.9053	49609.3201	28.9728	16787.98735
5	25.3769	48352.55685	29.4683	16481.30364
5	25.5524	49403.77421	34.7311	14065.43415
5	23.9519	51487.64816	29.4110	16715.14059
5	29.3046	41863.22284	33.7613	14428.4136
5	25.6540	48065.68177	32.6970	15108.51148
5	26.7251	46190.99648	30.7607	15992.51643
5	25.9071	46982.68042	34.0194	14347.04904
5	23.6806	51497.1749	32.2600	14964.01116
5	21.7299	56354.33205	36.1039	13626.39493
6	31.4497	39399.83529	38.7630	12685.70544
6	29.7587	41619.55999	41.4611	12054.14232
6	36.7043	33678.31562	36.4028	13470.17262
6	30.2337	40841.21361	42.7932	11443.26669
6	33.3747	37026.52009	37.3014	13271.03004
6	29.6625	41580.27813	39.3916	12531.22493
6	34.0746	36091.22337	38.8387	12850.43011
6	30.8406	40039.00702	36.7749	13328.79219
6	27.7709	44457.14759	40.0056	12283.30534
6	28.3396	43765.15547	38.4918	12775.94189
7	55.6127	22386.84689	72.6650	6783.898713
7	65.6757	18905.8358	73.8004	6753.24253
7	64.5209	19308.28615	74.8946	6679.827384
7	55.4759	22346.60456	76.4726	6564.351153
7	51.5427	23898.22419	75.8286	6596.086437
7	54.2398	22957.66209	68.9211	7251.059545
7	59.8739	20620.01974	77.3691	6426.312313
7	61.6284	20214.56017	73.4419	6782.681276
7	62.1940	20036.51478	73.3673	6931.153252
7	61.9129	20053.18762	74.4489	6701.401901
8	86.2489	14519.36199	93.1989	5389.52713
8	82.1298	15239.20672	89.3193	5719.088708
8	88.1192	14142.89962	89.2479	5633.746004
8	81.5629	15187.06422	87.6838	5760.961546
8	89.8048	13855.95202	89.9145	5556.790062
8	84.6081	14729.47626	91.4296	5548.40008
8	83.5707	14831.56178	86.6624	5937.592312
8	90.1089	13955.79127	86.4583	5913.081798
8	88.7447	13953.79104	87.7641	5676.614926
8	87.3729	14303.69142	86.7580	5890.580696
9	62.9521	19784.75698	62.0727	8092.73642
9	68.2903	18573.03307	69.4471	7141.507709
9	62.9250	19600.38141	63.6300	7999.622819
9	66.5845	18587.49409	65.1545	7739.127766
9	64.9861	19073.725	63.3421	7847.04012
9	65.3041	19127.48204	62.0482	8241.947389
9	60.9477	20438.40867	58.4628	8504.365169
9	63.9824	19262.42217	62.9387	7851.353778
9	64.0246	19314.62282	65.2555	7570.074553
9	60.8262	20401.6197	69.3413	7244.744474
10	78.4141	16266.95964	78.9922	6452.611777
10	90.8479	13659.01688	83.8903	5989.989307
10	88.4158	14027.49282	93.9932	5435.286808
10	83.7932	14930.42395	85.3519	5977.875126
10	87.5371	14300.74791	83.9862	6110.801536
10	85.1392	14641.26983	93.5937	5351.043927
10	90.1635	13799.94122	83.6697	6094.117703
10	93.0283	13454.97015	90.6841	5532.744991
10	83.3197	15081.97941	89.7265	5686.268828
10	89.3387	14060.17773	98.7057	5290.038974
Total	4563.1752	3933622.226	5095.0807	1205402.657

Appendix B Configuration Procedures

1. Testbed System Requirements

- **Server**

Operating System: Windows 2000 Advanced Server with Service Pack 3
Hardware:

Processor - AMD Athlon XP 1600+ 1.40GHz
Memory - 512 MB RAM
Network Card - Intel Pro/100 S Desktop network card

Software:

Orinoco AP-2000 software version 1.4 variant 1.47
Solariswind TFTP version 3
Ethereal version 0.9.5

- **Client**

Operating System: Windows XP Professional 2002

Hardware:

Processor - AMD Athlon XP 1600+ 1.40GHz
Memory- 512 MB of RAM
Network Cards - Intel Pro/100 S Desktop network card
Orinoco USB client

Software:

Orinoco USB client driver
Orinoco Client Manager version 1.7
WinHTTrack version 3.2

- **Access Point**

Hardware:

Orinoco AP-2000

Software:

Orinoco built-in functions

- **Firewall**

Operating System: Windows 2000 Advanced Server with Service Pack 3

Software:

Network ICE BlackICE version 2.9
Microsoft RAS - configure this machine as a router as well.

2. Server Functionality Enabling

This assumes the AD and DNS Server has already been enabled and has hotfixes of Q304347, Q304697, and Q306260[28] [Microsoft, 2002c].

[28] Please refer to Microsoft Knowledge Base for these hotfixes at: http://search.microsoft.com/gomsuri.asp?n=1&c=rp_BestBets&siteid=us&target=http://search.support.microsoft.com/kb/c.asp.

➢ **AD**

- Click on Property and edit Default Group Policy (domain).
- Create user groups according to their security functions, e.g. Wireless and VPN Groups.

✍ In Windows Configuration > enable reversible encrypted password[29] (see Figure b-1).

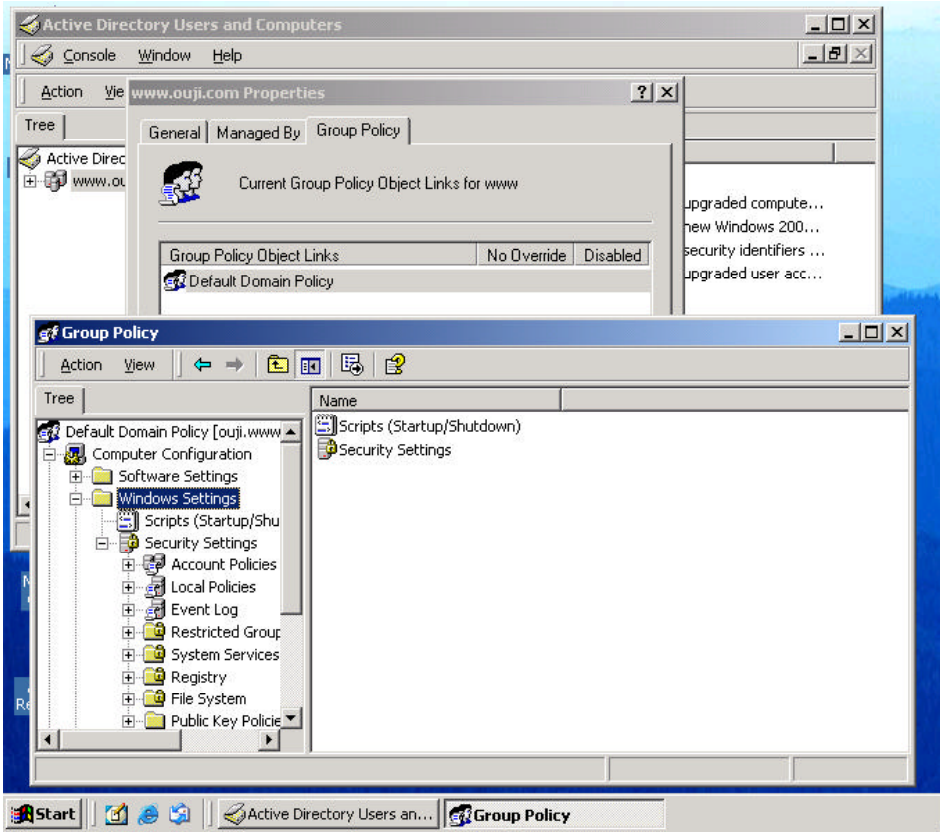

Figure b-1 Default Group Policy

✍ In the PKI configuration > enable automatic machine/computer certificates for automatic issuing of computer certificate.

➢ **DNS Server**

-Enable dynamic updates for zone in the Property section.

-Change to native mode if possible (better integration with remote access policies).

➢ **Certificate Authority (CA) Server**

- If the organisation has no previous CA in place, use Microsoft certificate server provided in the administrative tools.
- Choose root CA if that is the organisation's preferred CA, else choose the other options such as a child or sub domain CA from the list.
- Users can request certificates via the web interface before either 802.1X or VPN is in place[30].

[29] If users already exist in other groups, reset password and reissue digital certificates afterwards.
[30] Or users may choose to request certificates via wired connection.

➢ **IAS (RADIUS server) [Microsoft, 2000b, 2002a-b]**

- Accept RAS clients of (a) AP-2000 and (b) VPN server.
- Configure Client details with (a) and (b)'s information (see Figure b-2).

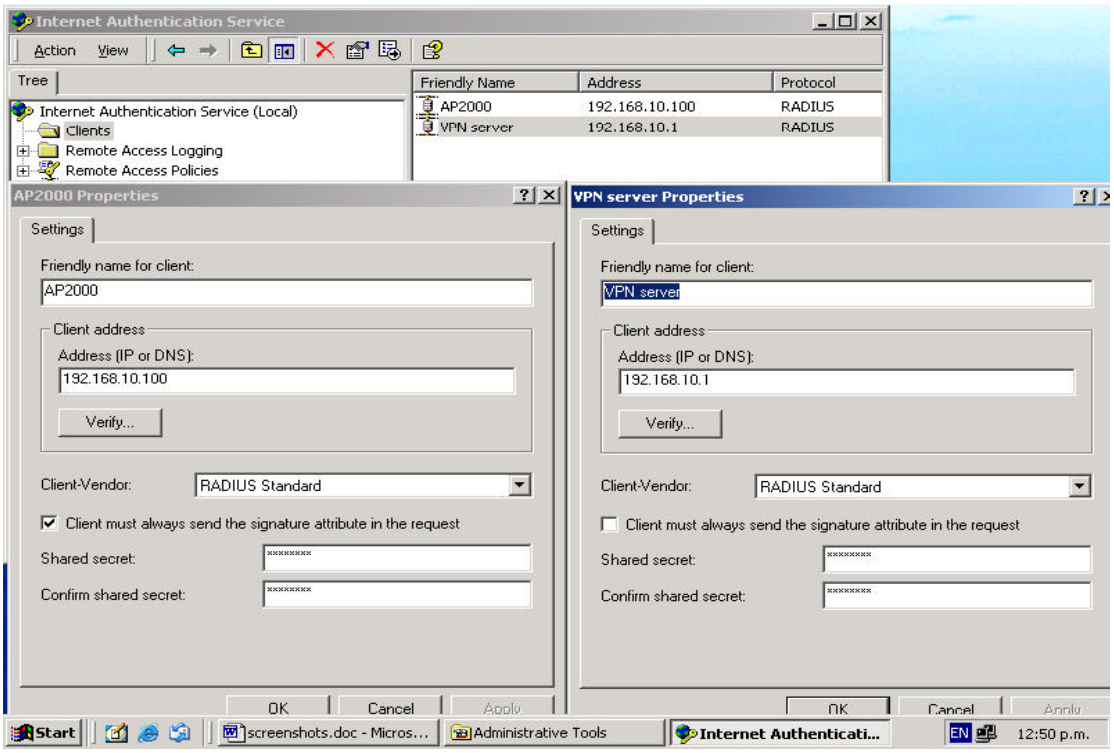

Figure b-2 RADIUS Client Configuration

- Configure Remote Access Policy (see Appendix C). Please note if you use the VPN server (RAS in Microsoft platform), you should still construct remote access policy in IAS instead of RAS.

➢ **IIS server**

- Enable IIS from Administrative tools; it provides FTP and Web server.
- For FTP server, select the timeout, e.g. 900 seconds.
- For Web server, administrators can provide unlimited timeout.

2.1 802.1X Model Configuration

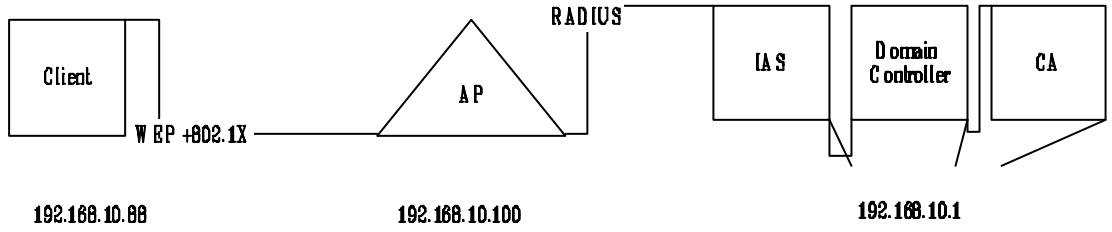

Figure b-3 Logical Components and IP address issuing

➢ **Client [Microsoft, 2002c-d]**

- Click WLAN connections' Property >select Authentication menu
  - ✍ WEP authentication (if enabled) becomes Shared key authentication.
  - ✍ WEP encryption provided either when the administrator has configured the WLAN NIC in advance or the user types in the secret key.

✎ Four keys can be selected at AP; therefore, if the user manually types in the password (thus automatic password option is not on), the user will need to select the right key number ranging from 0-3 (1-4 in AP).

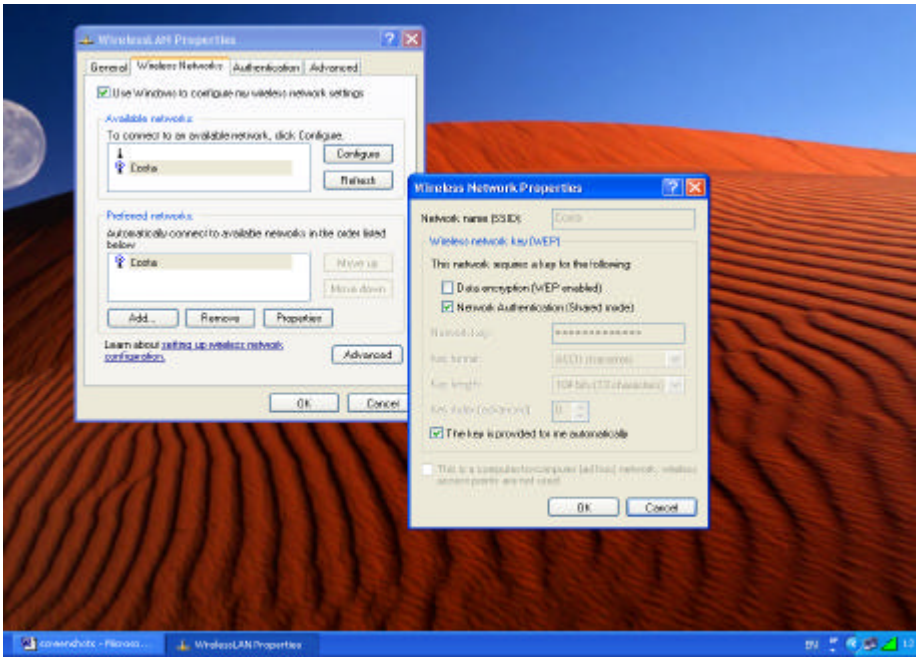

Figure WEP and Windows XP

- Click Property on the WLAN connection >select 802.1X panel >select either Certificate (smartcard) or MD5.

✍ If certificate is selected > select the CA to be trusted and enable verify server's certificate (see Figure b-4).

✎ After the network is connected, user will be automatically logged in to the organisation's network.

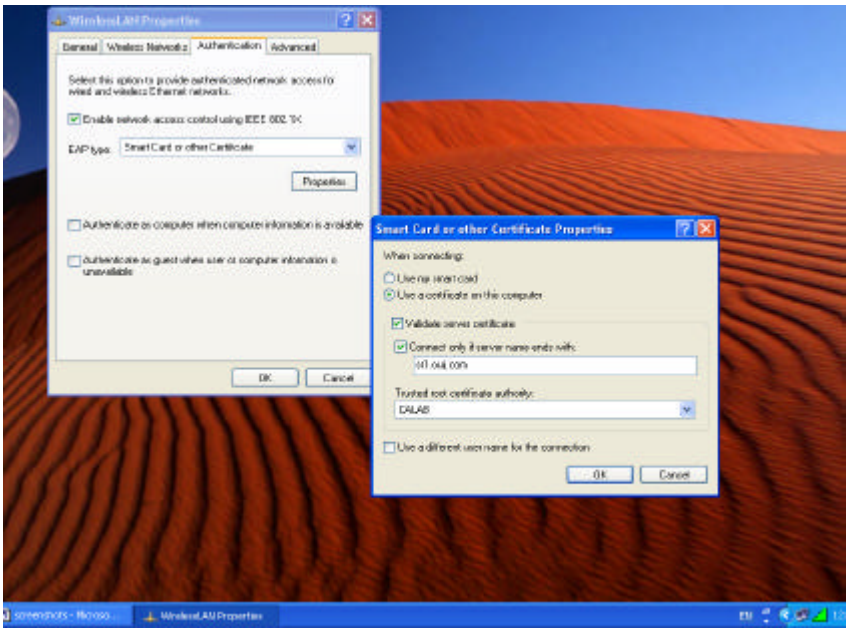

Figure b-4 802.1X and Windows XP

✍ If MD5 is selected when the wireless network is connected, a screen will appear asking the user to enter username and password (see Figure b-5). If the user is pre-Windows2000, use domain\user, else user@domain username.

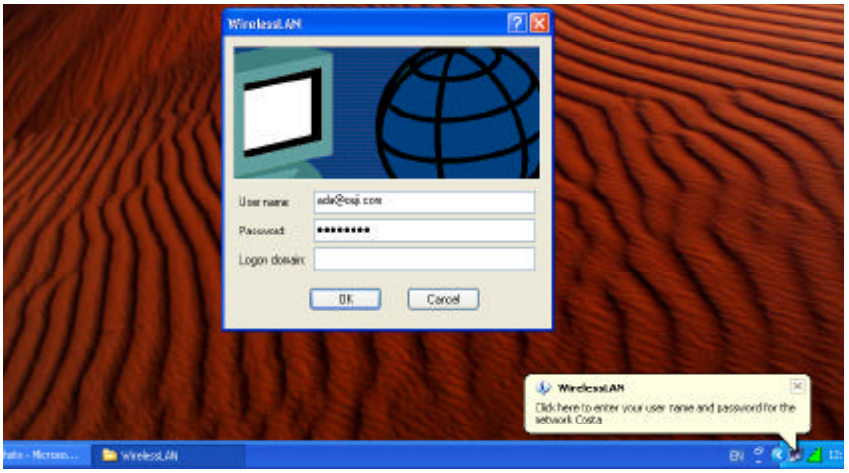

Figure b-5 EAP-MD5 Connection

➢ **Access Point**[31]

- For using the basic 802.11 security:

✍ Enable MAC address authentication and type in clients' NICs' MACs.

✍ For WEP authentication, select only the secret key number (see Figure b-6).

✍ Enable WEP encryption and select the secret key number.

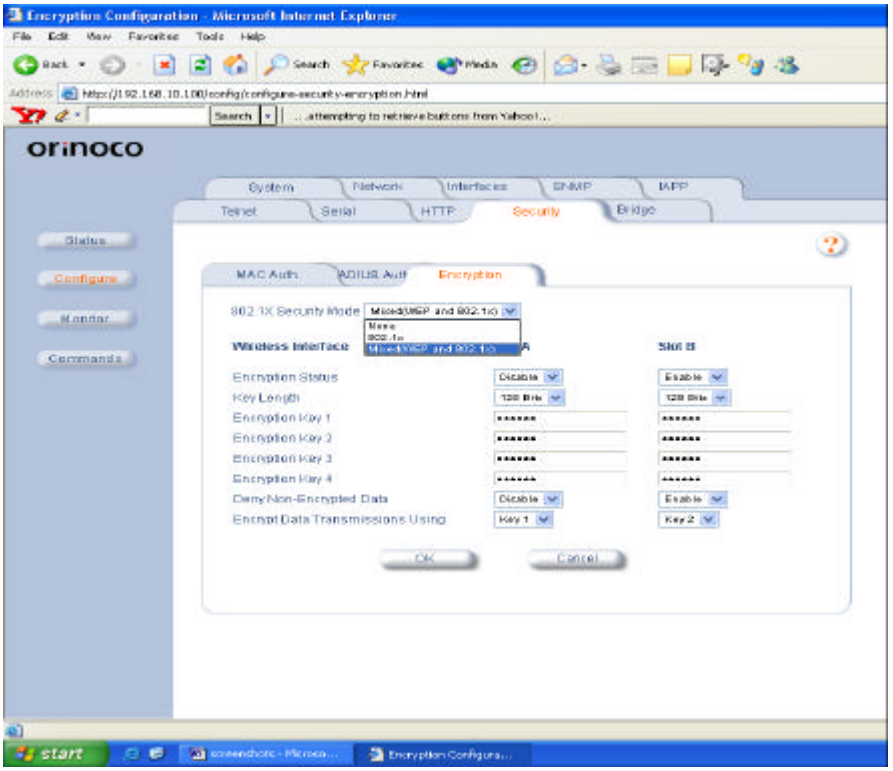

Figure b-6 WEP and AP-2000

[31] See Orinoco AP-2000 Guidebook.

- For the 802.1X standard protection (use with RADIUS, see [Microsoft, *Troubleshooting Windows XP IEEE 802.11 Wireless Access*, 2002] for troubleshooting):
  - For 802.1X authentication select only "802.1X mode"[32]:
    - Disable Encryption
    - Disable Deny unencrypted
    - Select key number 1
  - For 802.1X authentication and WEP encryption using "Mixed mode":
    - Enable encryption and "deny encryption"
    - Use key number 1
  - Enable RADIUS sever (see Figure b-7)

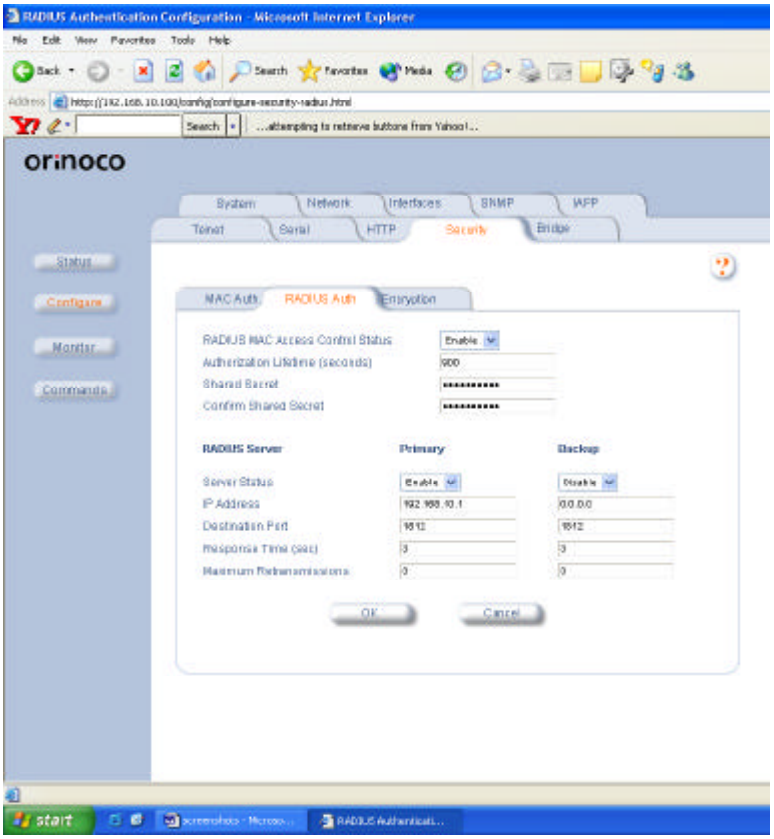

Figure b-7 RADIUS and AP-2000

- **<u>RADIUS Server</u>**

  - Configure the RADIUS client with AP's IP address, shared secret, and allow digital signature.
    - See remote policy configuration in Appendix C.

[32] Can select "Mixed mode" as long as encryption is not enabled.

2.2 VPN Model Configuration

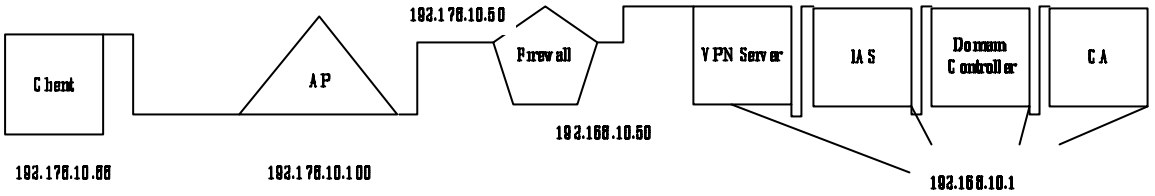

Figure b-8 Logical Components and IP address Issuing

➢ **Client (Different Subnetwork)**

- First dial-in WLAN connection (WEP and 802.1X disabled).
- Second dial-in VPN connection (IPSec and PPTP) with selected authentication and encryption (see Figure b-9 and b-10). For more information see Appendix C.

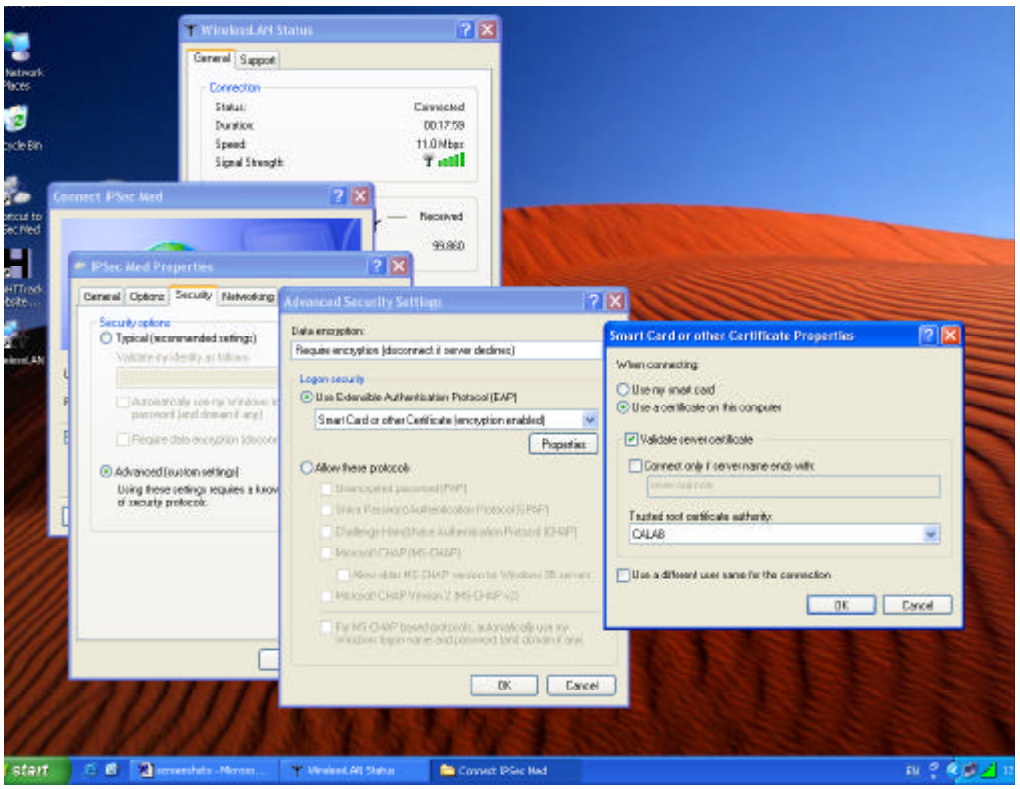

Figure b-9 IPSec EAP-TLS Dial-In

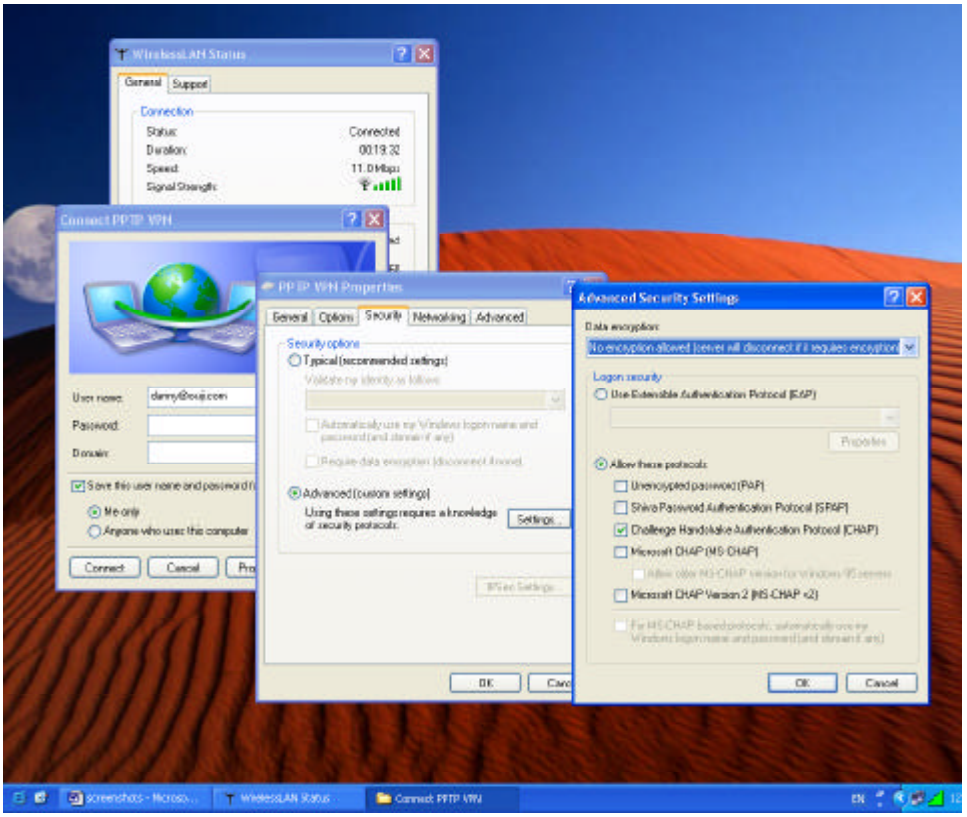

Figure b-10 PPTP CHAP Dial-in

- Enable IPSec Policy Management (if domain controlled then domain priority overrides local IPSec configuration). See Appendix C.

➢ **Access Point**

- Disable RADIUS
- Disable WEP encryption

➢ **IAS (RADIUS Sever)**

- Change RADIUS client to RAS, which uses IP addresses of 192.168.10.1.

➢ **RAS (VPN Server)**

- Configure Property with IP address, shared secret (see Figure b-11).
- Provide static IP address pool, such as 193.168.10.0-193.168.10.10, to be issued to users when access has been granted.
- Set security options.
- Enable IP routing.

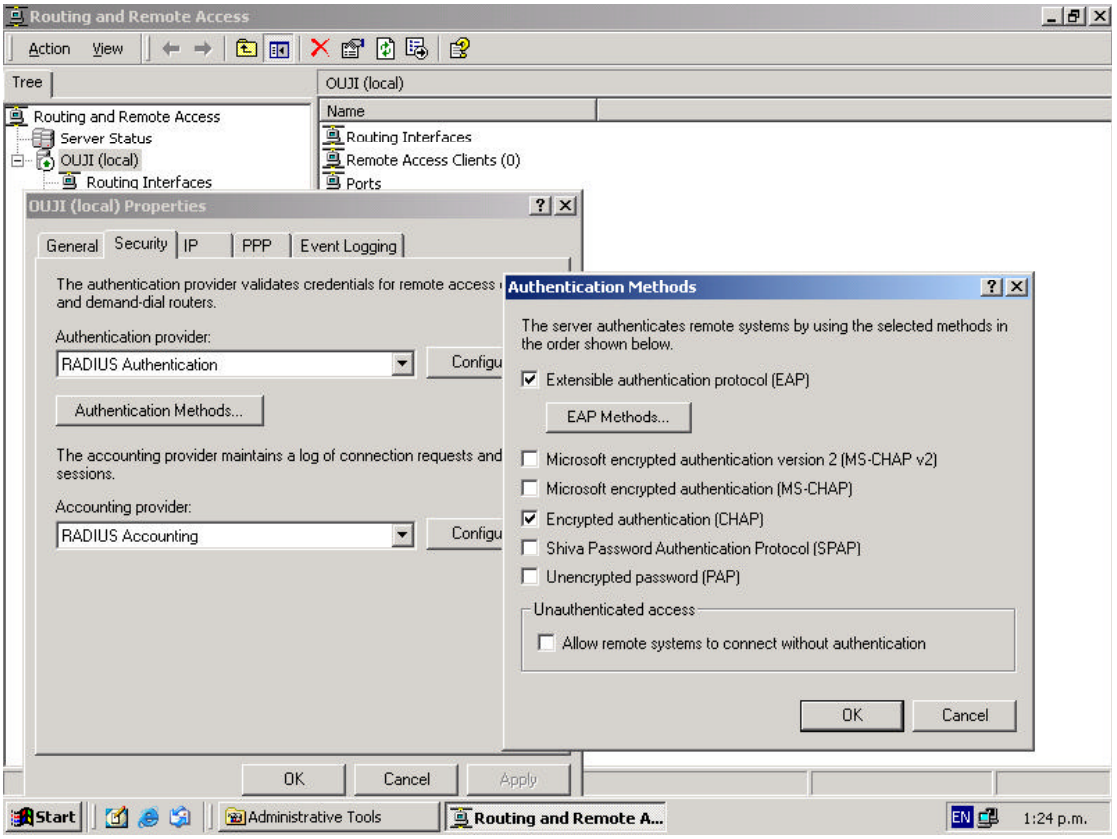

Figure b-11 RAS/VPN Server Property

- **IPSec Policy Management**

  - In the AD's Default Group Policy, enable IPSec Policy (default or customised).

Appendix C Remote Policy Activation

The following policies are configured in IAS remote access policies. Be sure the Account and Dial-in panels in users' Property in the AD has either "allow" or "control through remote policy" enabled (see Figure c-1).

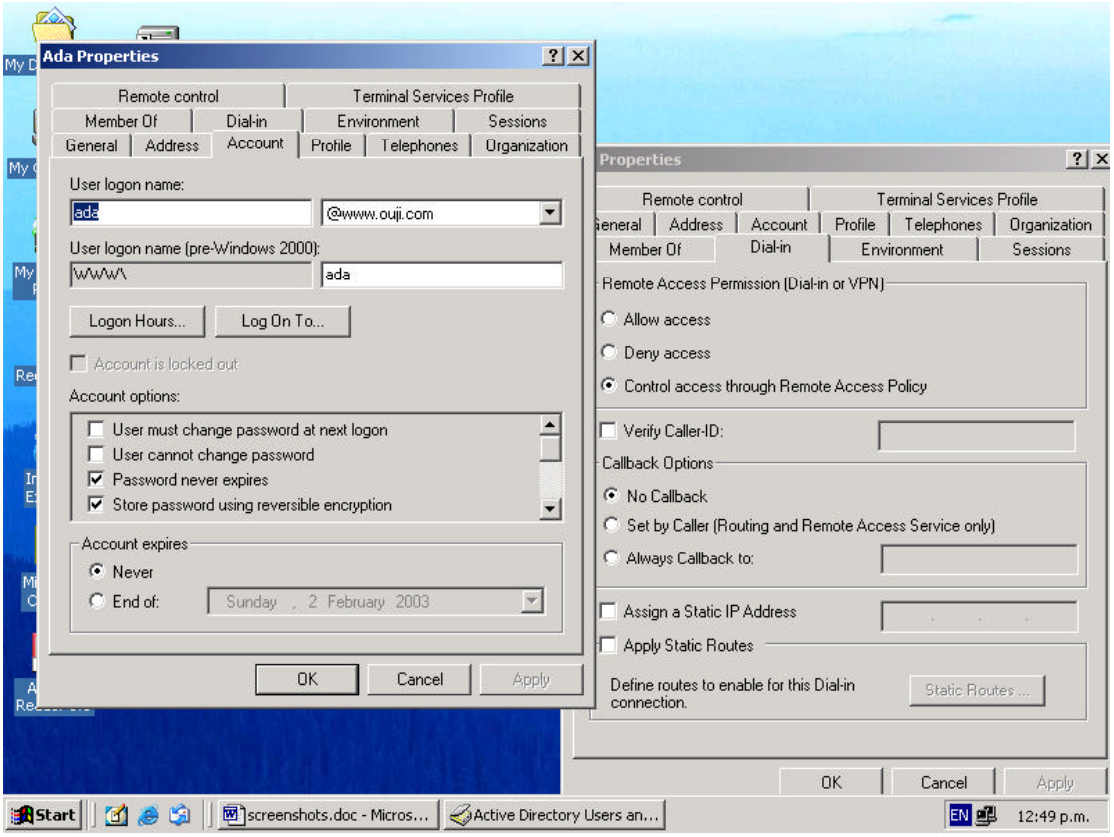

Figure c-1 User Property in AD

Add new remote access policy and then edit the "Profile" for security and other configurations. Remove the default remote access policy provided at the start.

1. 802.1X Model Policy Activation (see Figure c-2)

- **<u>Wireless via EAP-MD5 Enabled Policy</u>**
  - Add Wireless group or other groups that while using the WLAN.
  - Add RADIUS as the client-vendor specific support.
  - Select 802.11 as the NAS port.
  - For authentication selects EAP-MD5 (enable reversible encrypted password).

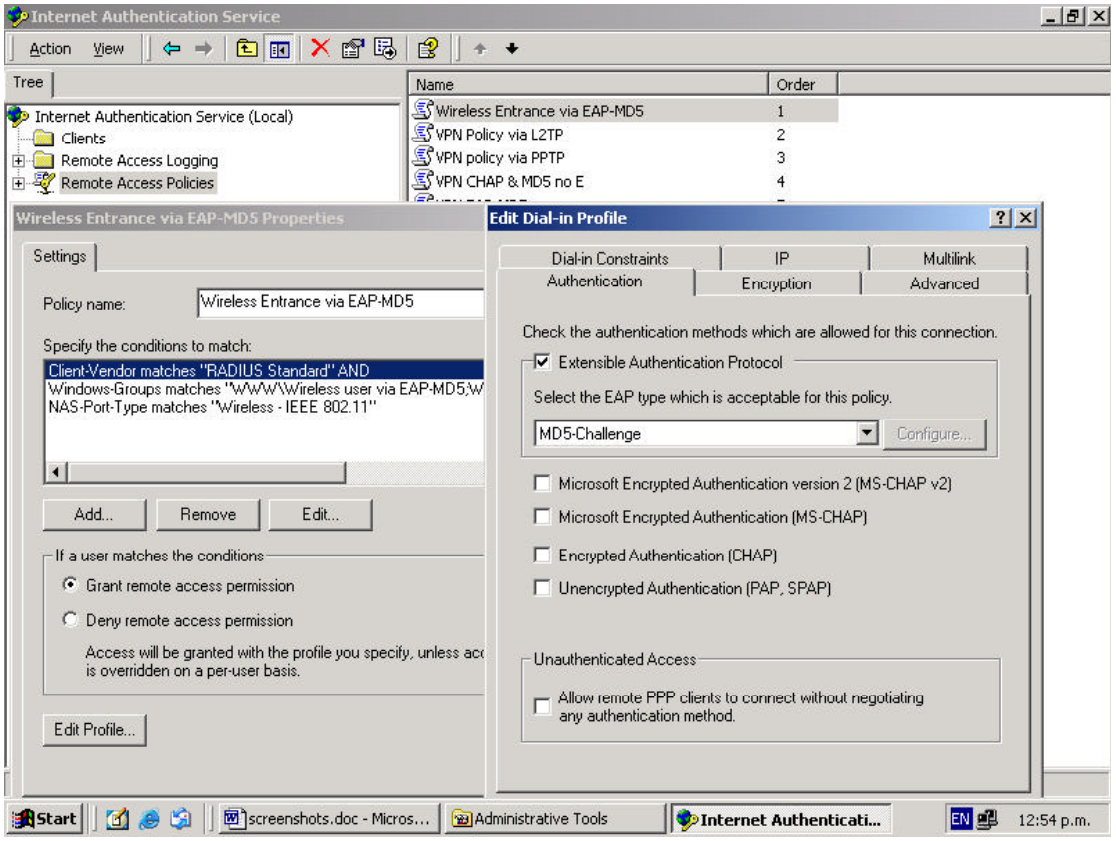

Figure c-2 802.1X Policy Example in IAS

- **<u>Wireless via EAP-TLS enabled Policy</u>**
  - Add Wireless group or other groups that should be using the WLAN
  - Add RADIUS as the client-vendor specific support
  - Select 802.11 as NAS port
  - For authentication selects EAP-TLS

1. VPN Model Policy Activation

We constructed a customised IPSec Policy to provide an HMAC-SHA1 hashing function; if users wish to use HMAC-MD5, there is no need to construct an IPSec Policy. Microsoft provides an IPSec policy, *L2TP Rule*, which is automatically created on remote RAS and L2TP/IPSec Dial-in. Administrators will need to disable this rule if customised policy configuration is desired (see Microsoft Knowledge Base Q310109).

1.1 IPSec Policy

The policy is called *SecureRemote* for the server and the client, and contains:

- A customised *Enforce* filter for all remote traffic with certificate-based authentication (see Figure c-3 for Policy Configuration and Figure c-4 for IPSec filter [Microsoft, 1999a, 2001]).
  - ESP [3DES, HMAC-SHA1]
  - ESP [DES, HMAC-SHA1]
  - ESP [No Confidentiality, HMAC-SHA1]

✍ Another filter to permit ICMP (ping) traffic.

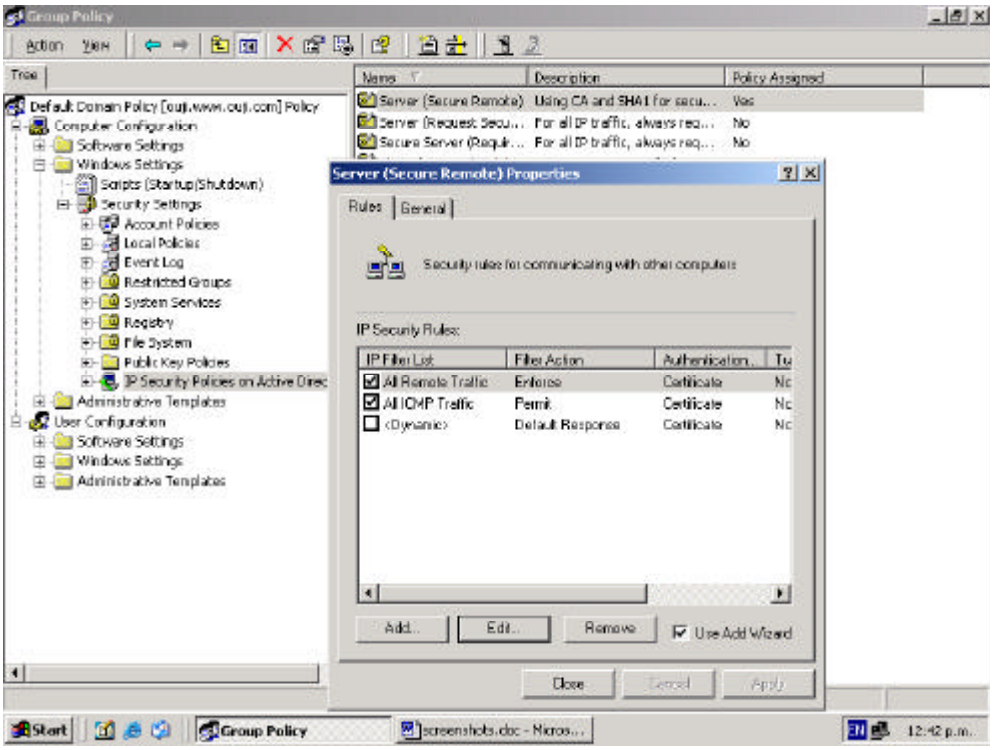

Figure c-3 IPSec Policy Configuration

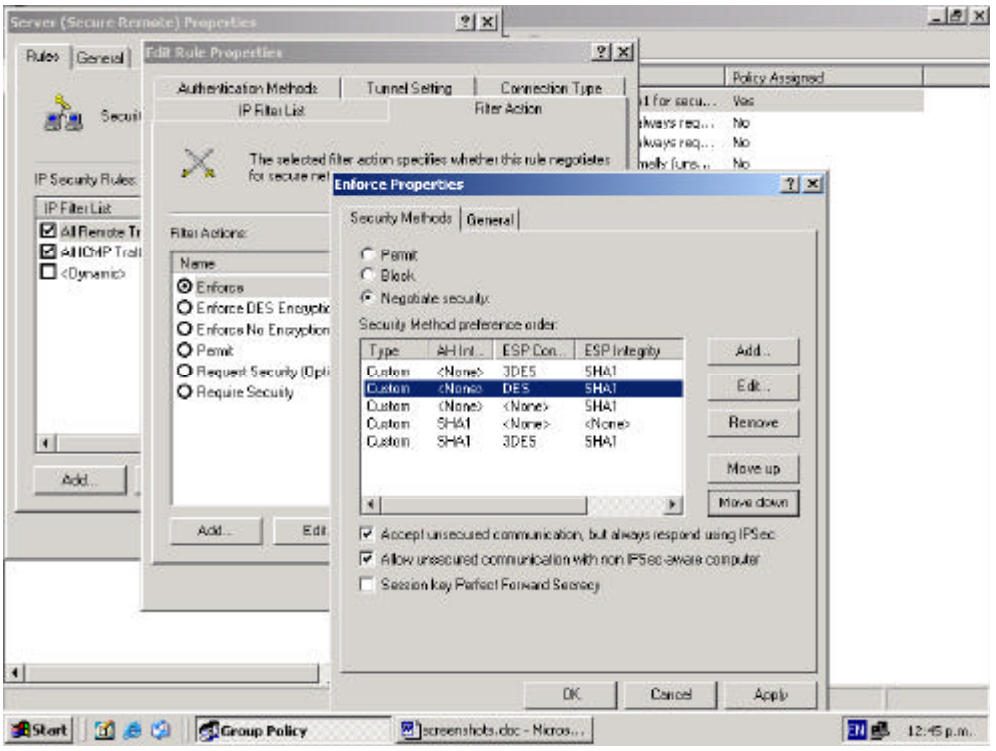

Figure c-4 IPSec Filter

1.2 Remote Access Policy

- **VPN Access Via IPSec Policy (Figure c-5)**
  - Add VPN group or other groups that will use the WLAN.
  - Add RADIUS as the client-vendor specific support.
  - Select VPN as the NAS port and L2TP/IPSec as tunnelling technology.
  - For authentication, select CHAP and EAP-TLS (other options can be selected if desired).
  - For encryption allow all ranges from No (0), Basic (40-bit MPPE), Strong (56-bit MPPE, DES) to Strongest (128-bit MPPE, 3DES).

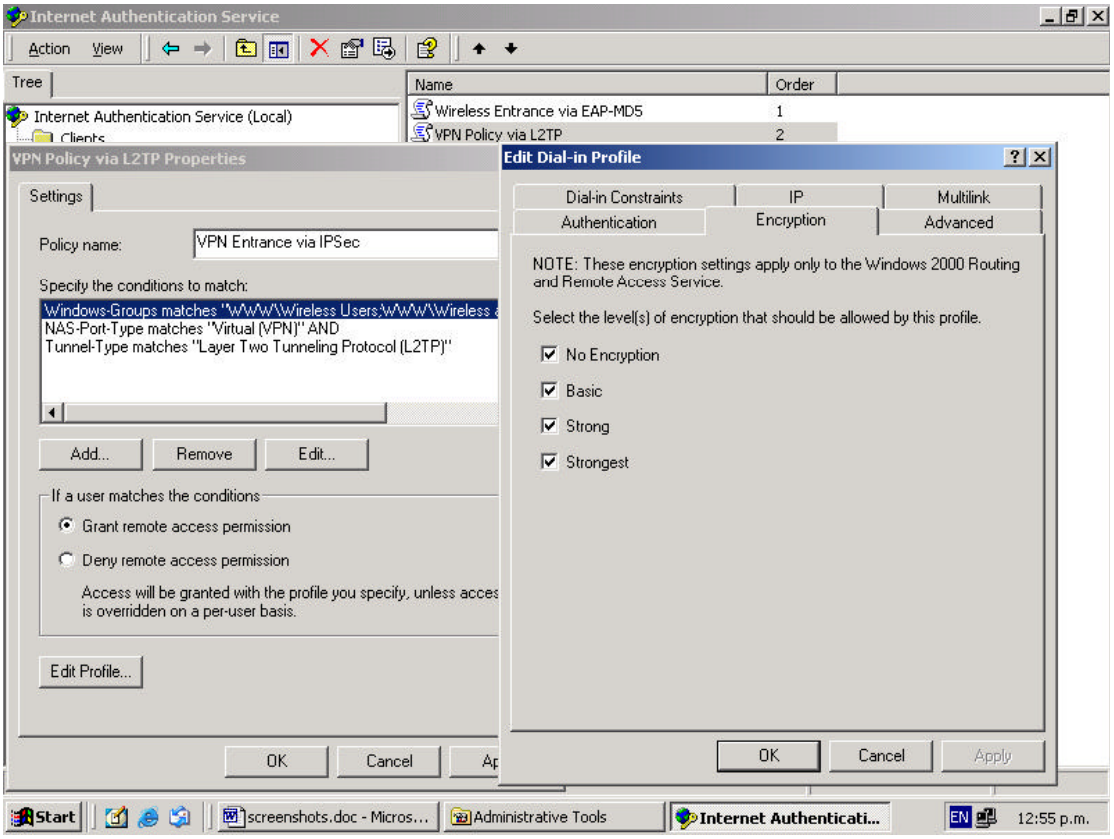

Figure c-5 VPN Policy and Property

- **VPN Access Via PPTP Policy**
  - Add VPN group or other groups that will use the WLAN.
  - Add RADIUS as the client-vendor specific support.
  - Select VPN as the NAS port and PPTP as tunnelling technology.
  - For authentication select CHAP and EAP-TLS (other options can be selected if desired).
  - For encryption allow all ranges from No (0), Basic (40-bit MPPE), Strong (56-bit MPPE, DES) to Strongest (128-bit MPPE, 3DES).

Acronyms and Abbreviations

NUMBER
1G First Generation
2G Second Generation
3DES Triple Data Encryption Standard
3G Third Generation

A
AAA Authentication, Authorisation, and Accounting
ACK Acknowledgment
ACL Access Control List
AD Active Directory
AES Advanced Encryption Standard
AH Authentication Header
AMPS Advanced Mobile Phone System
AP Access Point
ANOVA Analysis of Variance
AS Authentication Server
ATM Asynchronous Transfer Mode

B
BSS Basic Service Set

C
CCK Complementary Code Keying
CDP Cisco Discovery Protocol
CHAP Challenge Handshake Authentication Protocol
CRC Checksum
CDMA Code Division Multiple Access
CHAP Challenge Handshake Authentication Protocol
COPS Common Open Policy Service
CSMA/CA Carrier Senses Multiple Access with Collusion Avoidance
CTS Clear To Send

D
DCF Distributed Coordination Function
DF Degree of Freedom
DIAMETER
DoS Denial of Service
DDoS Distributed Denial of Service
DES Data Encryption Standard
DHCP Dynamic Host Control Protocol
DNS Domain Name Server
DS Distribution System
DSSS Direct Sequence Spread Spectrum

E
EAP Extensible Authentication Protocol
EAPOL EAP over LAN

EAPOW EAP over Wireless
EAP-SRP EAP Secure Remote Password
E-commerce Electronic Commerce
ESN Enhanced Security Network
ESP Encapsulating Security Protocol
ESS Extended Service Set
ETSI European Telecommunications Standard Institute

F

FDMA Frequency Division Multiple Access
FHSS Frequency-Hopping Spread Spectrum
FTP File Transfer Protocol

G

GHz Gigahertz
GPRS General Packet Radio
GPS Global Positioning System
GRE Generic Routing Encapsulation
GSM Global System for Mobile

H

HiperLAN High Performance Radio LAN
HTTP HyperText Transfer Protocol
HMAC Hashed Message Authenticated Code
HR/DSSS High Rate DSSS

I

IAPP Inter-Access Point Protocol
IAS Internet Authentication Server
IBSS Interdependent Basic Service Set
ICV Integrity Check Value
IDS Intrusion Detection System
IEEE Institute of Electrical and Electronics Engineers
IETF Internet Engineering Task Force
IIS Internet Information Service
IKE Internet Key Exchange
IP Internet Protocol
IPSec Internet Protocol Security
IR Infrared
IAS Internet Authentication Service
ISAKMP Internet Security Association and Key Management Protocol
ISM Industrial, Scientific, and Medical
ISO International Organization for Standardization
ISP Internet Service Provider
ITU International Telecommunication Union
IV Initialisation Vector

K

Kbps Kilobits per second

L

LLC Logical Link Layer
L2TP Layer 2 Tunnelling Protocol
LAN Local Area Network
LDAP Lightweight Directory Access Protocol

M

MAC Medium Access Control
MAN Metropolitan Area Network
Mbps Megabits per second
M-commerce Mobile Commerce
MD Message Digest
MHz Megahertz
MIB Management Information Base
MPEG Multimedia P
MPPE Microsoft Point-to-Point Encryption
MS-CHAP Microsoft CHAP

N

NAS Network Access Server
NAT Network Address Translation
NIC Network Interface Card

O

OFDM Orthogonal Frequency-Division Multiplexing
OSI Open Systems Interconnection
OTP One Time Password

P

PAE Port Access Entity
PAP Password Authentication Protocol
PAN Personal Area Network
PBNM Policy Based Network Management
PC Personal Computer
PCF Point Coordination Function
PDA Personal Digital Assistant
PDC Personal Digital Communication
PHY Physical Layer
PKCS Public Key Cryptography Standards
PKI Public Key Infrastructure
PKIX Public-Key Infrastructure X.509
PPP Point-to-Point Protocol
PPTP Point-to-Point Tunnelling Protocol
PRNG Pseudorandom Number Generator

Q

QoS Quality of Service

R

RADIUS Remote Authentication Dial-in User Service
RAS Remote Access Server

RC 4 Rivest Cipher 4
RF Radio Frequency
RFC Request for Comment
ROI Return On Investment
RSA Rivest Shamir Adelman
RTS Request To Send

S

SA Security Association
SHA Secure Hashed Algorithm
SIG Special Interest Group
S/MIME Secure Multi-Purpose Internet Mail Extensions
SNMP Simple Network Management Protocol
SPAP Shiva Password Authentication Protocol
SRP Secure Remote Password
SSID Service Set Identifier
SSL Secure Sockets Layer
SSH Secure Shell
STA Station
STP Spanning Tree Protocol

T

TA Transmitter Address
TACAS Terminal Access Controller Access Control System
TCP Transmission Control Protocol
TDMA Time Division Multiple Access
TFTP Trivial File Transfer Protocol
TG Task Group
TK Temporal Key
TKIP Temporal Key Integrity Protocol
TLS Transport Layer Security
TTLS Tunnelled TLS

U

UDP User Datagram Protocol
UMTS Universal Mobile Telecommunications Service

V

VPN Virtual Private Network

W

WDMZ Wireless Demilitarised Zone
WECA Wireless Ethernet Compatibility Alliance (Now known as Wi-Fi Alliance)
WEP Wired Equivalent Privacy
WEP2 Wired Equivalent Privacy 2
Wi-Fi Wireless Fidelity
Wi-Fi Alliance Wireless Fidelity Alliance
WIP Work in Progress
WLAN Wireless Local Area Network
WPAN Wireless Personal Area Network
WWAN Wireless Wide Area Network

References

Aboba, B., & D. Simon. (1999). *PPP EAP TLS Authentication Protocol*. RFC 2716. Internet Engineering Task Force. October.

Amaro, J., & R. P. Lopes. (2001). *Performance Analysis of a Wireless MAN*. Network Computing and Applications. pp.358-361, 8-10 October.

ANSI/IEEE. Std 802.11 (1999). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* New York. First Edition. Institute of Electrical and Electronics Engineers, Inc. ISBN 0-7381-1658-0. 20 August.

Arbaugh, W. A., N. Shankar, & Y. C. Wan. (2001). *Your 802.11 Wireless Network Has No Clothes*. University of Maryland. Maryland. 30 March.

Avery, M. (2001). *Putting 802.11b to the Test.* Network World. 02 May. http://www.nwfusion.com/reviews/2001/0205rev.html

Bansal, R. (2001). *Wireless Networks: An Electronic Battlefield?* IEEE Microwave Magazine. pp. 32-34, December.

Bing, B., & R. Subramanian. (1998). *A Novel Technique for Quantitative Performance Evaluation of Wireless LANs.* Computer Communications, 21. Elsevier. pp.833-838.

Blunk, L., & J. Vollbrecht. (1998). *PPP Extensible Authentication Protocol (EAP),* RFC2284: Internet Engineering Task Force.

Borisov, B., I. Goldberg, & D. Wagner. (2001*). Intercepting Mobile Communications: The Insecurity of 802.11*. Seventh Annual International Conference on Mobile Computing and Networking. ACM. 16-21 July.

Bradner, S. (1991). *Benchmarking Terminology for Network Interconnection Devices*. RFC 1242. Internet Engineering Task Force. July.

Bradner, S., & J. McQuaid. (1999). *Benchmarking Methodology for Network Interconnect Devices*. RFC 2544. Internet Engineering Task Force. March.

Brewin, B., & D. Verton. (2002). *Airport WLANs Lack Safeguards*. Computerworld. 16 September.

Briney, A., & F. Prince. (2002). *Does Size Matter?* Information Security Magazine, TruSecure Coporation. September.

Caballero, J., & D. Malmkvist. (2002). *Experimental Study of a Network Access Server for a Public WLAN Access Network*. Master Thesis, Department of Microelectronics and Information Technology, Royal Institute of Technology. KTH, Stockholm., January.

Calhoun, P., J. Arkko, G. Zorn, & J. Loughney. (2002). *DIAMETER Base Protocol*. Internet Draft. Internet Engineering Task Force. June.

Chen, J. C. (2001). *Measured Performance of 5-GHz 802.11a Wireless LAN Systems.* Atheros Communications, Inc. 27 August. http://www.atheros.com/AtherosRangeCapacityPaper.pdf

Chevillat, P., & W. Schott. (2001). *Wireless Access Technology Beyond 3G*. Paper presented at the Wireless World Research Forum (WWRF), Munich. 7 March.

Cisco. (1998). *Performance Management: Best Practices White Paper,* Cisco Systems, Inc. http://www.cisco.com/warp/public/126/perfmgmt.htm.

Common Criteria (1999). *Common Methodology for Information Technology Security Evaluation---Part2: Evaluation Methodology.* Version 1. Common Criteria. August. http://www.commoncriteria.org/docs/PDF/CEMV10.PDF

Computer Society. (2001). *A Long-Term View of Short-Range Wireless: Wireless PANs and LANs.* Computer Society, Institute of Electrical and Electronics Engineers, Inc. June. http://computer.org/computer/homepage/june/cover_feature/side01.htm

Congdon, P., B. Aboba, T. Moore, A. Smith, G. Zorn, & J. Roese. (2002). *IEEE 802.1X RADIUS Usage Guidelines.* Internet-Draft. Internet Engineering Task Force. 17 June.

Cooper, D.R. & P.S. Schindler (2001). *Business Research Methods.* Seventh Edition. McGraw-Hill. ISBN 0-07-118109-1.

Convery, S., & D. Miller. (2001). *SAFE: Wireless LAN Security in Depth.* Cisco Systems, Inc. December. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safw1_wp.pdf

Davies, J. (2001). *Virtual Private Networking with Windows 2000: Deploying Remote Access VPNs.* Microsoft. August.

Dierks, T., & C. Allen. (1999). *The TLS Protocol Version 1.0,* RFC 2246. Internet Engineering Task Force.

Enterasys Network. (2002). *Wireless Demilitarised Zone (WDMZ)-Enterasys Network's Best Practices Approach to an Interoperable WLAN Security Solution*. Enterasys Network. http://www.bitpipe.com/data/detail?id=1015306519_611&type=RES&x=187349215

Ethereal. (2002), *EtherealHomepage*, http://www.ethereal.com.

Finseth, C. (1993). An Access Control Protocol, Sometimes Called TACAS, RFC1492. Internet Engineering Task Force.

Fluhrer, S., I. Mantin, & A. Shamir. (2001). *Weaknesses in the Key Scheduling Algorithm of RC4.* Eighth Annual Workshop on Selected Areas in Cryptography, August.

Funk, P., & S. Blake-Wilson. (2002). *EAP Tunnelled TLS Authentication Protocol (EAP-TTLS).* Internet Draft. Internet Engineering Task Force. November.

Gast, M. (2002). *Chapter 15: 802.11 Network Deployment*, 802.11 Wireless Networks: The Definitive Guide. O'Reilly. ISBN 0-596-00183-5. April.

Geng, X., Y. Huang, & A. B. Whinston. (2002). *Defending Wireless Infrastructure against the Challenge of DDoS Attacks.* Mobile Networks and Applications, 7. Kluwer Academic. pp. 213-223, July.

Goth, G. (2002). *Wireless Security Still Ad Hoc and Add-On.* DS Online Exclusive. IEEE Distributed Systems Online, 3(7). 7 July. http://dsonline.computer.org/0207/features/news.htm

Halpern, J., S. Convery, & R. Saville. (2001). *SAFE VPN: IPSec Virtual Private Networks in Depth.* Cisco System Inc. http://www.mnemonic.no/linker/pdf/IPSec_VPN_in_Depth.pdf

Hamzeh, K., G. Pall, W. Verthein, J. Taarud, W. Little, & G. Zorn. (1999). *Point-to-Point Tunnelling Protocol (PPTP).* RFC2637, Internet Engineering Task Force. July.

Hannikainen, M., T. D. Damalainen, M. Niemi, & J. Saarinen. (2002). *Trends in Personal Wireless Data Communications*. Computer Communications, 25. Elsevier. pp.84-99.

Hansen, J. V. (2001). *Internet Commerce Security: Issues and Models for Control Checking*. The Journal of the Operational Research Society, 52(10). pp.1159-1164. October.

Harkins, D., & D. Carrel. (1998). *The Internet Key Exchange (IKE).* RFC 2409. Internet Engineering Task Force. November.

Harris, B. A. (1998). *Firewall and Virtual Private Networks.* Master Thesis, Department of Computer Science. University of Canterbury. Christchurch.

Held, G. (2001). *The ABCs of IEEE 802.11*. IT Professional, 3(6). Institute of Electrical and Electronics Engineers, Inc. pp.49-52. November.

HiperLAN. (2002). *HiperLAN/2 Standard*.http://www.hiperlan2.com

HomeRF (2002), *HomeRF Homepage.* http://www.homerf.org.

Housley, R., & D. Whiting. (2001). *IEEE P802.11 Wireless LANs: Temporal Key Hash.* Document Number: IEEE 802.11-01/550r3. IEEE Task Group I. 20 December. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/1-550.zip

Housley, R., D. Whiting, & N. Ferguson. (2002). *IEEE P802.11 Wireless LANs: Alternate Temporal Key Hash.* Document Number: IEEE 802.11-02/282r2. IEEE Task Group I. 23 April. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-282.zip

Hunt, R. (2001). *Technological Infrastructure for PKI and Digital Certification.* Computer Communications, 24. Elsevier. pp.1460-1471. December.

IEEE Std. 802.1X (2001). *Port-Based Network Access Control.* New York. Institute of Electrical and Electronics Engineers, Inc. ISBN 0-7381-2627-5. 25 October.

IEEE 802.11 WG. (2002). 802.11 Working Group. http://www.ieee802.org/11.

IEEE Std. 802.11a (1999). Supplement to ANSI/IEEE. Std 802.11, 1999 Edition. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) in the 5 GHz band.* Institute of Electrical and Electronics Engineers, Inc.

IEEE Std. 802.11b (1999). Supplement to ANSI/IEEE. Std 802.11, 1999 Edition. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band.* Institute of Electrical and Electronics Engineers, Inc. ISBN 0-7381-1811-7. September.

IEEE. Std. 802.11f/D3.1. (2002). Draft Supplement to ANSI/IEEE. Std. 802.11, *Draft: Recommended Practice for Multi-Vendor Access Point Interoperability Via an Inter-Access Point Protocol across Distribution Systems Supporting IEEE 802.11 Operation*. Institute of Electrical and Electronics Engineers, Inc. September.

InterLink Networks. (2001). *Wireless LAN Access Control and Authentication*. InterLink Networks. http://www.interlinknetworks.com/references/WLAN_Access_Control.html

Jain, R., K. K. Ramakrishnan, & D. M. Chiu. (1997). *Congestion Avoidance in Computer Networks with a Connectionless Network Layer*. Digital Equipment Corporation. June.

Karygiannis, T., & L. Owens. (2002). *Draft: Wireless Network Security - 802.11, Bluetooth and Handheld Devices.* USA. National Institute of Standards and Technology.

Kent, S., & R. Atkinson. (1998*). Security Architecture for the Internet Protocol.* RFC 2401. Internet Engineering Task Force, November.

King, M. (2000). *Will the Enterprise Perimeter Survive?,* Business Communication Review (pp. 12-17)

Lee, Y.-J. (2002). *Mobile IP and AAA Architecture for Wireless LAN*. Master's Thesis. Department of Electrical Engineering. National Taiwan University. Taipei. June.

Lenzini, L., & E. Mingozzi. (2001). *Performance Evaluation of Capacity Request and Allocation Mechanisms for Hiperlan2 Wireless LANs.* Computer Networks, 37(1). pp.5-15,

Maier, P. (2000). *Ensuring Extranet Security and Performance*. Information Systems Management, 17(2). pp.33-40, Spring.

Maughan, D., M. Schertler, M. Schneider, & J. Turner. (1998). *Internet Security Association and Key Management Protocol (ISAKMP).* RFC2408. Internet Engineering Task Force.

McDonough, J. (2002*). Wireless LANs That Tell All*. Wireless NewsFactor.13 March. http://www.wirelessnewsfactor.com/perl/story/16748.html

Microsoft. (1999a). *Microsoft Privacy Protected Network Access: Virtual Private Networking and Intranet Security.* Microsoft. 13 May. http://www.microsoft.com/windows2000/docs/nwpriv.doc

Microsoft. (1999b). *Online Help Book,* Windows 2000 Advanced Server software. Microsoft.

Microsoft. (2000a). *Chapter 5 Overview of Performance Monitoring*, Windows 2000 Resource Kit, CD-ROM. Microsoft.

Microsoft. (2000b). *Internet Authentication Service for Windows 2000*. Microsoft. 1 June, http://www.microsoft.com/windows2000/docs/IAS.doc

Microsoft. (2002a). *Enterprise Deployment of IEEE 802.11 Using Windows XP and Windows 2000* Internet Authentication Service. Microsoft. http://www.microsoft.com/windowsxp/pro/techinfo/deployment/wireless/default.asp

Microsoft. (2002b*). RADIUS Protocol Security and Best Practices*. Microsoft. 17 January. http://www.microsoft.com/windows2000/techinfo/administration/radius.asp

Microsoft. (2002c). *Troubleshooting Windows XP IEEE 802.11 Wireless Access*. Microsoft. http://www.microsoft.com/windowsxp/pro/techinfo/administration/networking/troubleshooting.asp

Microsoft. (2002d). *Wireless 802.11 Security with Windows XP*. Microsoft. http://www.microsoft.com//windowsxp/pro/techinfo/administration/wirelesssecurity/XP80211Security.doc

Mitton, D., M. St.Johns, S. Barkley, D. Nelson, B. Patil, M. Stevens, & B. Wolff. (2001). *Authentication, Authorisation, and Accounting: Protocol Evaluation*. RFC3127. Internet Engineering Task Force. June.

O'Hara, B., & A. Petrick. (1999). *The IEEE 802.11 Handbook: A Designer's Companion.* New York. The Institute of Electrical and Electronics Engineers, Inc. ISBN 0-7381-1855-9.

Orinoco. (2002). *Principles of 802.1X Security.* ORiNOCO Technical Bulletin 048/B. Lucent. April.

Patel, B., B. Aboba, W. Dixon, G. Zorn, & S. Booth. (2001). *Securing L2TP Using IPSec.* RFC3193. Internet Engineering Task Force. November.

Rigney, C., W. Willats, & P. Calhoun. (2000). *RADIUS Extensions,* RFC 2869: Internet Engineering Task Force. June.

Rigney, C., W. Willats, A. Rubens, & W. Simpson. (2000). *Remote Authentication Dial in User Service (RADIUS),* RFC2865: Internet Engineering Task Force. June.

Rincon, R. B. (2002). *Secure WLAN Operation and Deployment in Home and Small to Medium Size Office Environment*. Master's Thesis, Department of Engineering and Computer Science. Technische Universitat Berlin. Berlin. 6 March.

Rodgers, C. (2001). *Virtual Private Networks: Strong Security at What Cost?* Department of Computer Science. University of Canterbury. Christchurch. November.

Roshan, P. (2001). *802.1X Authenticates 802.11 Wireless.* Network World Fusion. 24 September.

Schneider, B. (2002). *Fixing Network Security by Hacking the Business Climate.* Paper presented at the IT Security NZ 2002, Wellington. 7-8 August.

Seng, N., T. (2002). *Secured Public Access WLAN,* APRICOT (Asia Pacific Regional Internet Conference on Operational Technologies, Bangkok. 27 February - 27 March.

SIG. (2000). *Special Interest Group*, Bluetooth. http://www.bluetooth.org.

Simpson, W. (1996). *PPP Challenge Handshake Authentication Protocol (CHAP).* RFC1334. Internet Engineering Task Force. August.

Stubblefield, A., J. Ioannidis, & A. D. Rubin. (2001). Using the Fluhrer, Mantin, and Shamir *Attack to Break WEP*: AT&T Lab Technical Report TD-4ZCPZZ.

Task Group i. (2002). *TGi Security Overview*, Institute of Electrical and Electronics Engineers, Inc. Document number IEEE 802.11-02/114r1.

TGg. (2002). *Task Group 802.11g*, http://grouper.ieee.org/groups/802/11/index.html

TGi. (2002). *Task Group 802.11i*: Institute of Electrical and Electronics Engineers, Inc. http://www.ieee802.org/11.

Thayer, R., N. Doraswamy, & R. Glenn. (1998). IP Security Document Roadmap. RFC2411. Internet Engineering Task Force. November.

Townsley, W., A. Valencia, G. Pall, G. Zorn, & B. Palter. (1999). *Layer Two Tunnelling Protocol"L2TP"*. RFC 2661. Internet Engineering Task Force. August.

Walke, B. H. (2002). *Mobile Radio Networks: Networking, Protocols and Traffic Performance*. Second Edition. ISBN 0471-499021. John Wiley & Son Ltd.

Walker, J. R. (2000). *Unsafe at Any Key Size; an Analysis of the WEP Encapsulation*. Tech. Rep. 03628E. IEEE. 802.11 Committee. March. http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

Wearden, G. (2002). *Heard of Drive-by Hacking?* Meet Drive-by Spamming. ZDNetUK. 5 September.

Weatherspoon, S. (2000). *Overview of IEEE 802.11b Security.* Intel Technology Journal, Q2.

WECA. (2001a). *802.11b Wired Equivalent Privacy (WEP) Security*: WECA. 19 February. http://www.wi-fi.org/WI-FiWEPSecurity.pdf.

WECA. (2001b). *Wireless LAN Research Study. Survey.* WECA. http://wi-fi.org/pptfiles/Wireless_LANResearch_ExecutiveSummary.ppt

Weyuker, E. J., & A. Avritzer. (2002). *A Metric for Predicting the Performance of an Application under a Growing Workload*. IBM Systems Journal, 41(1). pp.45-54.

Whitmore, J. J. (2001). *A Method for Designing Secure Solutions*. IBM Systems Journal, 40(3). pp.747-768.

Wong, J. (2001). *Policy Based Network Management*. Department of Accountancy, Finance, and Information Systems. University of Canterbury. Christchurch. October.

Wu, T. (2000). *The SRP Authentication and Key Exchange System*. RFC 2945. Internet Engineering Task Force. September.

Xiao, Y., & J. Rosdahl. (2002). *Throughput Limit for IEEE 802.11*. IEEE 802.11 Working Group. May. Document Number: IEEE 802.11-02/291r0.

Yang, S. J. (2001). *An Approach to Modelling Performance Evaluation on the Ethernet with QoS Parameters*. International Journal of Network Management, 11. John Wiley & Sons, Ltd. pp.91-101.